IEC 62280

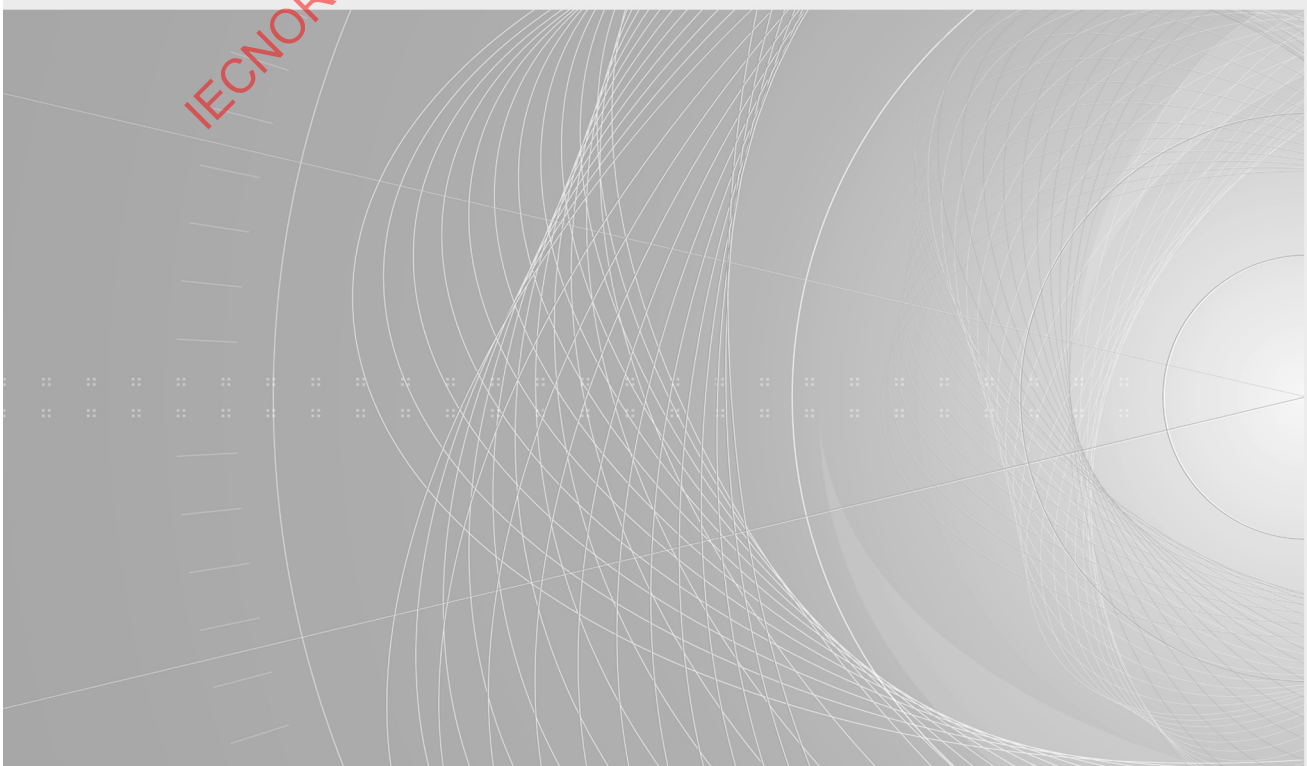
Edition 1.0 2014-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Railway applications – Communication, signalling and processing systems – Safety related communication in transmission systems

Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Communication de sécurité dans les systèmes de transmission



IEC 62280:2014-02(EN-FR)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

IEC 62280

Edition 1.0 2014-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Railway applications – Communication, signalling and processing systems – Safety related communication in transmission systems

Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Communication de sécurité dans les systèmes de transmission

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX XB

ICS 45.060

ISBN 978-2-8322-1383-4

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

RAILWAY APPLICATIONS – COMMUNICATION, SIGNALLING AND PROCESSING SYSTEMS – SAFETY RELATED COMMUNICATION IN TRANSMISSION SYSTEMS

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62280 has been prepared by IEC technical committee 9: Electrical equipment and systems for railways.

This standard is based on EN 50159.

This standard cancels and replaces IEC 62280-1 (2002) and IEC 62280-2 (2002). See Annex E.

The text of this standard is based on the following documents:

FDIS	Report on voting
9/1866A/FDIS	9/1885/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

INTRODUCTION

If a safety related electronic system involves the transfer of information between different locations, the transmission system then forms an integral part of the safety related system, this includes that the end to end communication is safe in accordance with IEC 62425.

The transmission system considered in this standard, which serves the transfer of information between different locations, has in general no particular preconditions to satisfy. It is from the safety point of view not trusted, or not fully trusted.

The standard is dedicated to the requirements to be taken into account for the communication of safety related information over such transmission systems.

Although the RAM aspects are not considered in this standard it is recommended to keep in mind that they are a major aspect of the global safety.

The safety requirements depend on the characteristics of the transmission system. In order to reduce the complexity of the approach to demonstrate the safety of the system, transmission systems have been classified into three categories:

- Category 1 consists of systems which are under the control of the designer and fixed during their lifetime.
- Category 2 consists of systems which are partly unknown or not fixed, however unauthorised access can be excluded.
- Category 3 consists of systems which are not under the control of the designer, and where unauthorised access has to be considered.

The first category was previously covered by IEC 62280-1:2002, the others by IEC 62280-2:2002.

When safety related communication systems, which have been approved according to the previous standards, are subject of maintenance and/or extensions, informative Annex E can be used for traceability purposes of (sub)clauses of this standard with the (sub)clauses of the former series.

RAILWAY APPLICATIONS – COMMUNICATION, SIGNALLING AND PROCESSING SYSTEMS – SAFETY RELATED COMMUNICATION IN TRANSMISSION SYSTEMS

1 Scope

This International Standard is applicable to safety related electronic systems using for digital communication purposes a transmission system which was not necessarily designed for safety related applications and which is

- under the control of the designer and fixed during the lifetime, or
- partly unknown or not fixed, however unauthorised access can be excluded, or
- not under the control of the designer, and also unauthorised access has to be considered.

Both safety related equipment and non-safety related equipment can be connected to the transmission system.

This Internaitonal Standard gives the basic requirements needed to achieve safety related communication between safety related equipment connected to the transmission system.

This International Standard is applicable to the safety requirement specification of the safety related equipment connected to the transmission system, in order to obtain the allocated safety integrity requirements.

Safety requirements are generally implemented in the safety related equipment, designed according to IEC 62425. In certain cases these requirements may be implemented in other equipment of the transmission system, as long as there is control by safety measures to meet the allocated safety integrity requirements.

The safety requirement specification is a precondition of the safety case of a safety related electronic system for which the required evidence is defined in IEC 62425. Evidence of safety management and quality management has to be taken from IEC 62425. The communication related requirements for evidence of functional and technical safety are the subject of this standard.

This International Standard is not applicable to existing systems, which had already been accepted prior to the release of this standard.

This International Standard does not specify

- the transmission system,
- equipment connected to the transmission system,
- solutions (e.g. for interoperability),
- which kind of data are safety related and which are not.

A safety related equipment connected through an open transmission system can be subjected to many different IT security threats, against which an overall program has to be defined, encompassing management, technical and operational aspects.

In this International Standard however, as far as IT security is concerned, only intentional attacks by means of messages to safety related applications are considered.

This International Standard does not cover general IT security issues and in particular it does not cover IT security issues concerning

- ensuring confidentiality of safety related information,
- preventing overloading of the transmission system.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 62278 (all parts), *Railway applications – Specification and demonstration of reliability, availability, maintainability and safety (RAMS)*

IEC 62425:2007, *Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1.1
absolute time stamp
time stamp referenced to a global time which is common for a group of entities using a transmission system

3.1.2
access protection
processes designed to prevent unauthorised access to read or to alter information, either within user safety related systems or within the transmission system

3.1.3
additional data
data which is not of any use to the ultimate user processes, but is used for control, availability, and safety purposes

3.1.4
authentic message
message in which information is known to have originated from the stated source

3.1.5
authenticity
state in which information is valid and known to have originated from the stated source

3.1.6
closed transmission system
fixed number or fixed maximum number of participants linked by a transmission system with well known and fixed properties, and where the risk of unauthorised access is considered negligible

3.1.7
communication
transfer of information between applications

3.1.8
confidentiality
property that information is not made available to unauthorised entities

3.1.9
corrupted message
type of message error in which a data corruption occurs

3.1.10
cryptographic techniques
producing output data, calculated by an algorithm using input data and a key as a parameter

Note 1 to entry: By knowing the output data, it is impossible within a reasonable time to calculate the input data without knowledge of the key. It is also impossible within a reasonable time to derive the key from the output data, even if the input data are known.

3.1.11
cyclic redundancy check
cyclic code, used to protect messages from the influence of data corruption

3.1.12
data
part of a message which represents some information

Note 1 to entry: See also definitions 3.1.64: user data, 3.1.3: additional data and 3.1.42: redundant data.

3.1.13
data corruption
alteration of data

3.1.14
defence
measure incorporated in the design of a safety related communication system to counter particular threats

3.1.15
delayed message
type of message error in which a message is received at a time later than intended

3.1.16
deleted message
type of message error in which a message is removed from the message stream

3.1.17
double time stamp
case when two entities exchange and compare their time stamps. In this case the time stamps in the entities are independent of each other

3.1.18
error
deviation from the intended design which could result in unintended system behaviour or failure

3.1.19
failure
deviation from the specified performance of a system

Note 1 to entry: A failure is the consequence of a fault or an error in the system.

3.1.20
fault
abnormal condition that could lead to an error in a system

Note 1 to entry: A fault can be random or systematic.

3.1.21
feedback message
response from a receiver to the sender, via a return channel

3.1.22
hacker
person trying deliberately to bypass access protection

3.1.23
hazard
condition that can lead to an accident

3.1.24
hazard analysis
process of identifying hazards and analysing their causes, and the derivation of requirements to limit the likelihood and consequences of hazards to an acceptable level

3.1.25
implicit data
additional data that is not transmitted but is known to the sender and receiver

3.1.26
information
representation of the state or events of a process, in a form understood by the process

3.1.27
inserted message
type of message error in which an additional message is implanted in the message stream

3.1.28
integrity
state in which information is complete and not altered

3.1.29
manipulation detection code
function of the whole message without secret key

Note 1 to entry: In contrast to a MAC there is no secret key involved. By the whole message is meant also any implicit data of the message which is not sent to the transmission system. MDC is often based on a hash function.

3.1.30
masqueraded message
type of inserted message in which a non-authentic message is designed to appear to be authentic

3.1.31
message
information which is transmitted from a sender (data source) to one or more receivers (data sink)

3.1.32
message authentication code
cryptographic function of the whole message and a secret or public key

Note 1 to entry: By the whole message is meant also any implicit data of the message which is not sent to the transmission system.

3.1.33
message enciphering
transformation of bits by using a cryptographic technique within a message, in accordance with an algorithm controlled by keys, to render casual reading of data more difficult. Does not provide protection against data corruption

3.1.34
message errors
set of all possible message failure modes which can lead to potentially dangerous situations, or to reduction in system availability. There can be a number of causes of each type of error

3.1.35
message integrity
message in which information is complete and not altered

3.1.36
message stream
ordered set of messages

3.1.37
non-cryptographic safety code
redundant data based on non-cryptographic functions included in a safety related message to permit data corruption to be detected by the safety related transmission function

3.1.38
open transmission system
transmission system with an unknown number of participants, having unknown, variable and non-trusted properties, used for unknown telecommunication services and having the potential for unauthorised access

3.1.39
public network
network with unknown users, especially not under control of the railways

3.1.40
random failure
failure that occurs randomly in time

3.1.41
redundancy check
type of check that a predefined relationship exists between redundant data and user data within a message, to prove message integrity

3.1.42
redundant data
additional data, derived, by a safety related transmission function, from the user data

3.1.43
relative time stamp
time stamp referenced to the local clock of an entity. In general there is no relationship to clocks of other entities

3.1.44
repeated message
type of message error in which a single message is received more than once

3.1.45
re-sequenced message
type of message error in which the order of messages in the message stream is changed

3.1.46
safe fall back state
safe state of a safety related equipment or system as a deviation from the fault-free state and as a result of a safety reaction leading to a reduced functionality of safety related functions, possibly also of non-safety related functions

3.1.47
safety
freedom from unacceptable levels of risk

3.1.48
safety case
documented demonstration that the product (e.g. system/sub-system/equipment) complies with the specified safety requirements

3.1.49
safety code
redundant data included in a safety related message to permit data corruptions to be detected by the safety related transmission function

3.1.50
safety integrity level
number which indicates the required degree of confidence that a system will meet its specified safety functions with respect to systematic failures

3.1.51
safety reaction
safety related protection taken by the safety process in response to an event (such as a failure of the transmission system), which may lead to a safe fall back state of the equipment

3.1.52
safety related
carries responsibility for safety

3.1.53
safety related transmission function
function incorporated in the safety related equipment to ensure authenticity, integrity, timeliness and sequence of data

3.1.54
sequence number
additional data field containing a number that changes in a predefined way from message to message

3.1.55
source and destination identifier
identifier which is assigned to each entity. This identifier can be a name, number or arbitrary bit pattern. This identifier will be used for the safety related communication. Usually the identifier is added to the user data

3.1.56
systematic failure
failure that occurs repeatedly under some particular combination of inputs, or under some particular environmental condition

3.1.57
threat
potential violation of safety

3.1.58
time stamp
information concerning time of transmission attached to a message by the sender

3.1.59
timeliness
state in which information is available at the right time according to requirements

3.1.60
transmission code
redundant information, added to the safety and non-safety message of the non-trusted transmission system in order to ensure the integrity of the message during transmission

3.1.61
transmission system
service used by the application to communicate message streams between a number of participants, who may be sources or sinks of information

3.1.62
trusted
which has properties used as evidence to support the safety demonstration

3.1.63
unauthorised access
situation in which user information or information within the transmission system is accessed and/or changed by unauthorised persons or hackers

3.1.64
user data
data which represents the states or events of a user process, without any additional data. In case of communication between safety related equipment, the user data contains safety related data

3.1.65
valid message
message whose form meets in all respects the specified user requirements

3.1.66
validity
state of meeting in all respects the specified user requirements

3.2 Abbreviations

BCH Bose, Ray-Chaudhuri, Hocquenghem Code

BME Basic Message Errors

BSC Binary Symmetric Channel

CAN	Controller Area Network
CRC	Cyclic Redundancy Check
EC	European Community
ECB	Electronic CodeBook mode
EMI	Electromagnetic Interference
FTA	Fault Tree Analysis
GPRS	General Packet Radio Service
GSM-R	Global System for Mobile communication – Railways
HE	Hazardous Events
HW	Hardware
IT	Information Technology
LAN	Local Area Network
MAC	Message Authentification Code
MDC	Manipulation Detection code
MD4, MD5	Message Digest algorithms
MH	Main Hazard
MTBF	Mean Time Between Failures
MVB	Multi-purpose Vehicle Bus
PROFIBUS	Process Field Bus
QSC	q-nary symmetric channel
RAMS	Reliability, Availability, Maintainability and Safety
SIL	Safety Integrity Level
SR	Safety Related
SRS	Safety Requirements Specifications
SW	Software
TX	Transmission
UTC	Universal Coordinated Time
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity

4 Reference architecture

This International Standard defines the safety requirements for the safe communication between safety related equipment via a transmission system, which can either be closed or open. Both, safety related and non-safety related equipment can be connected to the transmission system. This clause describes possible configurations of the safety related

communication in transmission systems including the definition of involved functional blocks. Particular requirements to be fulfilled by these blocks are specified in further clauses.

A combined view – open and closed transmission system – of the principal architecture is shown in Figure 1, where all communication elements are linked according to the information flow to exchange safety related information between safety related equipment. The reference architecture also shows a non-safety related interface which is not always present. A typical use could be for diagnostic messages routed to a maintenance centre.

Besides the source and destination of safety related communication the reference architecture deals with a safety related communication system, which can be divided into

- safety related transmission functions incorporated in the safety related equipment. These functions ensure authenticity, integrity, timeliness and sequence of data,
- safety related cryptographic techniques which protect the safety related message. These can either be realised by incorporating them in the safety related equipment or having them outside of the safety related equipment but checked by safety techniques. These techniques protect the safety related message in a Category 3 transmission system and are not needed in the case of a Category 1 or 2 transmission system,
- a non-safety related, open or closed transmission system which may itself include transmission protection functions and/or access protection functions.

The characteristics of closed transmission systems (Category 1) are as follows:

- the number of pieces of connectable equipment – either safety related or not – to the transmission system is known and fixed;
- the risk of unauthorized access is considered negligible;
- the physical characteristics of the transmission system (e.g. transmission media, environment according to design hypothesis, etc.) are fixed and unchanged during the life cycle of the system.

The open transmission system (Category 2 and/or 3) can contain some or all of the following:

- elements which read, store, process or re-transmit data produced and presented by users of the transmission system in accordance with a program not known to the user. The number of users is generally unknown, and safety related and non-safety related equipment, and equipment which is not related to railway applications, can be connected to the open transmission system;
- transmission media of any type with transmission characteristics and susceptibility to external influences, which are unknown to the user;
- network control and management systems capable of routing (and dynamically re-routing) messages via any path made up from one or more than one type of transmission media between the ends of open transmission system, in accordance with a program not known to the user;
- other users of the transmission system, not known to the safety related application designer, sending unknown amounts of information, in unknown formats.

The open transmission system of Category 3 may be subject to unauthorised access to the transmission system for malicious purposes.

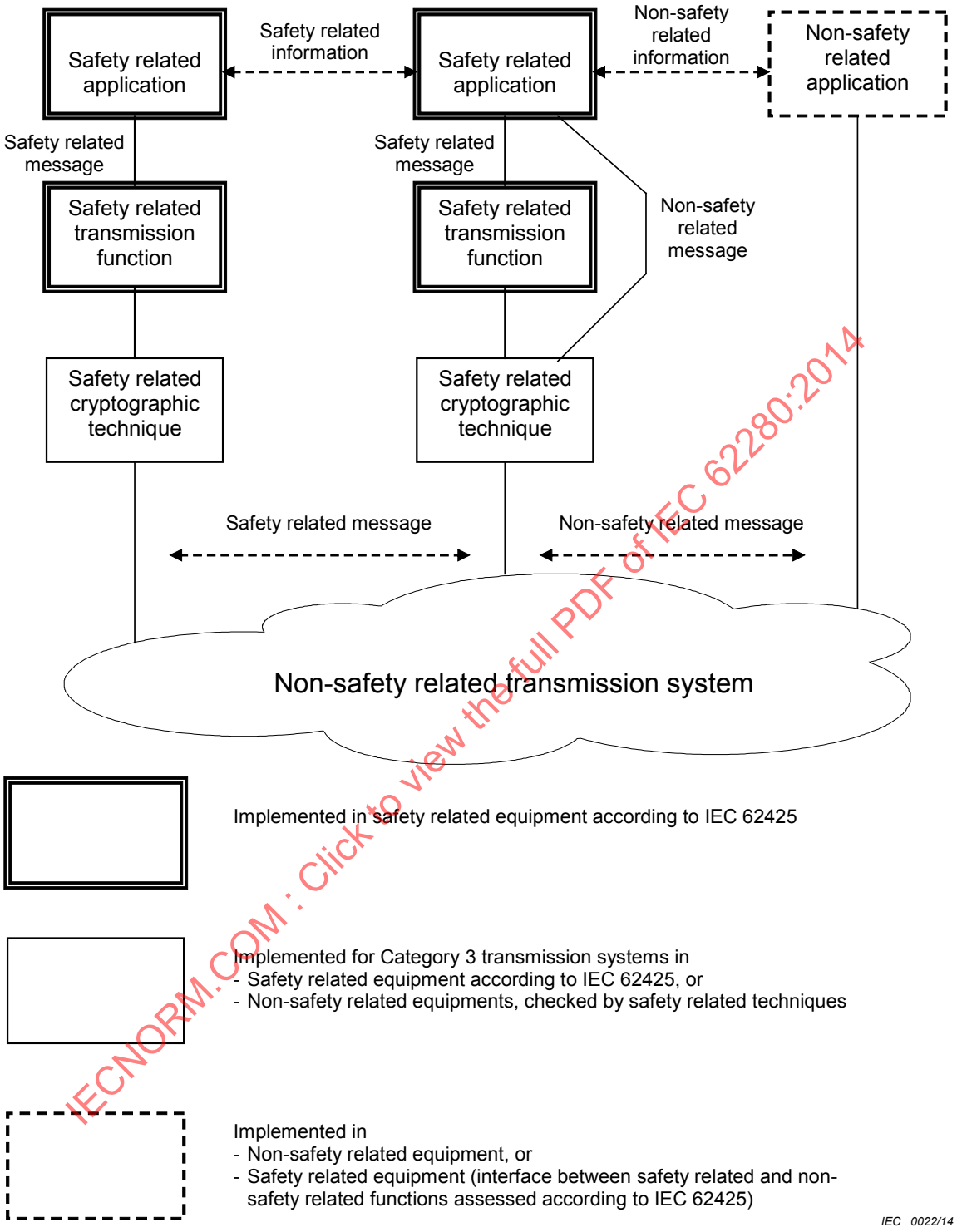


Figure 1 – Reference architecture for safety related communication

The reference architecture is not intended to restrict implementations; different structures are possible, see examples in the informative Annex C and in particular Clause C.5 for non-safety related messages.

5 Threats to the transmission system

The main hazard to safety related communication is the failure to obtain a valid message in terms of authenticity, integrity, sequence and timeliness at the receiving end. This standard considers threats to these message properties arising from the transmission system. Threats to the safety related equipment shall be considered in accordance with IEC 62425.

However, meeting the requirements of this standard does not give protection against intentional or unintentional misuse coming from authorised sources. It is necessary for the safety case to address these aspects.

Further information, with guidelines on threat analysis and safety case, is included in informative Annex A. It shall be emphasised that an analysis shall be made for each project, so although the methodology for message errors of Annex A can be included, it will not on its own necessarily be complete.

Hazardous events identified may include the following:

- systematic failure;
- broken wires;
- cabling errors;
- antenna misalignment;
- performance loss;
- HW random failure and ageing;
- human error;
- maintenance error;
- EMI;
- cross-talk;
- thermal noise;
- fading effects;
- overloading of transmission system;
- magnetic storm;
- fire;
- earthquake;
- lightning

as well as deliberately-caused events such as

- wire-tapping,
- damage or unauthorised change to HW,
- unauthorised change to SW,
- monitoring of channels,
- transmission of unauthorised messages.

However, although there can be a wide range of hazardous events, the basic message errors, which form the threats to the transmission system, are one of the following:

- repetition;
- deletion;

- insertion;
- re-sequencing;
- corruption;
- delay;
- masquerade.

Table A.1 suggests which threats to the transmission system can be caused by each type of hazardous event. Having identified the hazardous events – not protected by other means – that can occur for a particular system, the table can be used as a guide to identify the threats to be considered for that system.

Table A.1 does not contain probabilities of occurrence; this shall be part of analysis of threats.

6 Classification of transmission systems

6.1 General

This clause defines the process to be used to classify all transmission systems, identifying the threats relevant for such systems that affect the choice of defences for inclusion in the safety application.

6.2 General aspects of classification

There are many factors which can influence the threats to a safety related communication system.

For example it is possible that transmission services can be obtained by the signalling system user from private or public telecommunications service providers. Under such service provision contracts, the responsibility of the service provider for guaranteeing performance of the transmission system can be limited.

Therefore the significance of threats (and hence the requirements for defences) depend on the extent of control exercised by the user over the transmission system, including the following issues:

- the technical properties of the system, including guarantees of reliability or availability of the system, the extent of storage of data inherent in the system (which could affect delay or re-sequencing of messages);
- the consistency of the performance of the system over its life (e.g. as changes to the system, and changes to the user base are made), and traffic loading effects of other users;
- access to the system, depending on whether the network is private or public, the degree of access control exerted by the operator over other users, the opportunity for misuse of the system by other users, and the access available to maintainers to reconfigure the system, or gain access to the transmission medium itself.

Following these issues three categories of transmission systems can be defined.

6.3 Criteria for the classification of transmission systems

6.3.1 Criteria for Category 1 transmission systems

A transmission system can be considered to be of Category 1 if the following preconditions are fulfilled.

Pr1 The number of pieces of connectable equipment – either safety related or not – to the transmission system is known and fixed. As the safety related communication depends

on this parameter, the maximum number of participants allowed to communicate together shall be put into the safety requirement specification as a precondition. The configuration of the system shall be defined/ embedded in the safety case. Any subsequent change to that configuration shall be preceded by a review of their effects on the safety case.

Pr2 The characteristics of the transmission system (e.g. transmission media, environment under worst case conditions, etc.) are known and fixed. They shall be maintained during the life cycle of the system. If major parameters which were used in the safety case are to be changed, all safety related aspects shall be reviewed.

Pr3 The risk of unauthorised access to the transmission system shall be negligible.

If a transmission system satisfies all the above preconditions, it may be considered as Category 1 and a closed system and, if so, it shall comply with a generally reduced set of processes and requirements given in Clause 7.

6.3.2 Criteria for Category 2 transmission systems

If a transmission system does not satisfy the preconditions 1 or 2 (Pr1 or Pr2) of 6.3.1, but fulfils precondition 3 (Pr3) it shall be considered as Category 2 and an open system, and shall be assessed with a more comprehensive set of processes and requirements given in Clause 7.

6.3.3 Criteria for Category 3 transmission systems

If a transmission system does not satisfy the precondition 3 (Pr3) of 6.3.1 it shall be considered as Category 3 and an open system, and shall be assessed with the full set of processes and requirements given in Clause 7.

6.4 Relationship between transmission systems and threats

The significance of threats to the safety related communication system shall be assessed according to the extent of control exercised by the user over the transmission system.

The threats identified in Clause 5 are applicable to all the transmission systems categories with the exception of masquerade, which is only applicable to open transmission systems.

In Annex B an example of classification of transmission systems is given in Table B.1 and an example of threat/category relationship is given in Table B.2.

The applicability of Clause 7 depends on the category of the transmission system.

7 Requirements for defences

7.1 General

Certain techniques have been adopted in data transmission systems (non-safety related, safety related) in the past. These techniques form a “library” of possible methods accessible to the control and protection system designer, to provide protection against each threat identified above.

To reduce the risk associated with the threats identified in the preceding clause, the following fundamental safety services shall be considered and provided to the extent needed for the application, for both open and closed transmission systems:

- message authenticity;
- message integrity;
- message timeliness;

- message sequence.

The following set of known defences has been outlined:

a) sequence number;
b) time stamp;
c) time-out;
d) source and destination identifiers;
e) feedback message;
f) identification procedure;
g) safety code;
h) cryptographic techniques.

A number of architectural issues shall be considered by the particular application and justified in the safety case, for example

- conditions for claiming and maintaining the compliance with preconditions of Category 1 or 2 transmission systems,
- criteria for the separation among transmission systems of different categories,
- robustness of transmission systems against denial of service resulting from flooding attacks, e.g. need of firewalls.

With reference to h), the scope of this standard excludes general IT security issues:

- only attacks during the operational phase are considered;
- only attacks by means of messages to safety related applications are addressed here.

However, a complete access protection policy should consider

- procedural and maintenance aspects of access protection,
- vulnerability of software not part of the safety related application,
- confidentiality of information.

7.2 General requirements

7.2.1 Adequate defences shall be provided against all identified threats to the safety of systems using an open or closed transmission system. Any assumptions of threats which are to be ignored shall be justified and recorded in the safety case. Annex A provides a possible list of threats, to be used as guidance.

7.2.2 In case of communication between safety related and non-safety related applications via the same transmission system the following requirements apply:

- the safety defences implemented in the safety related transmission functions shall be demonstrated as being functionally independent from defences used by the non-safety related functions;
- the safety related and non-safety related messages shall have different structures achieved by applying a safety code to safety related messages. This safety code shall be capable of protecting the system to the required safety integrity (see 7.3.8) so that a non-safety related message cannot be corrupted into a safety related one.

7.2.3 Detailed requirements for the defences needed for the application shall take into account

- the level of risk (frequency/consequence) identified for each particular threat, and
- the safety integrity level of the data and process concerned.

Annex C gives guidance on the selection of currently known techniques to give defence against threats. Issues of effectiveness addressed in this annex should be carefully considered when the defence is chosen.

7.2.4 The requirements for the defences needed shall be included in the system requirements specification and in the system safety requirements specification for the application, and shall form input to the “assurance of correct operation” portion of the safety case for the application.

7.2.5 All defences shall be implemented according to the requirements defined in IEC 62425. This implies that the defences

- shall be implemented completely in the safety related transmission equipment (with the possible exception of some cryptographic architectures, see 7.3.9 and Clause C.2),
- shall be functionally independent from the layers used in the non-trusted transmission system.

7.2.6 Mandatory requirements for particular defences are given in the following subclauses. They apply when the particular defence is used.

7.2.7 Other defences than those described in this standard may be used, provided that analysis of their effectiveness against threats is included in the safety case.

7.2.8 The evidence of functional and technical safety shall follow the same process as specified in IEC 62425, including

- an overall error model,
- a functional specification based on analysis of the overall error model,
- analysis of each defence used in the safety related communication,
- the safety reaction in case of a detected transmission error,
- a safety integrity requirement specification and SIL allocation.

7.2.9 Subclause 7.3 defines a comprehensive set of defences. However for Category 1 transmission systems, the following reduced set is sufficient, still maintaining the fundamental safety services:

- source and/or destination identifiers (in case of more than one sender and/or more than one receiver);
- sequence number and/or time stamps to the extent needed by the application; and
- a safety code.

7.3 Specific defences

7.3.1 General

The following subclauses show short introductions and the requirements for specific defences, which are effective either alone or in combination against single or combined threats. All general requirements listed above shall be applied.

More detailed descriptions of the defences and the relation with all possible threats are given in informative Annex C.

7.3.2 Sequence number

7.3.2.1 General

Sequence numbering consists of adding a running number (called sequence number) to each message exchanged between a transmitter and a receiver. This allows the receiver to check the sequence of messages provided by the transmitter.

7.3.2.2 Requirements

The safety case shall demonstrate the appropriateness in relation to the safety integrity level of the process, and the nature of the safety related process, of the following:

- the length of the sequence number;
- the provision for initialisation and roll-over of the sequence number;
- the provision for recovery following interruption of the sequence of the messages.

7.3.3 Time stamp

7.3.3.1 General

When an entity receives information, the meaning of the information is often time-related. The degree of dependence between information and time can differ between applications. In certain cases old information can be useless and harmless and in other cases the information could be a potential danger for the user. Depending on the behaviour in time of the processes which interchange information (cyclic, event controlled, etc.) the solution may differ.

One solution which covers time-information relationships is to add time stamps to the information. This kind of information can be used in place of or combined with sequence numbers depending on application requirements. Different uses of time stamps and their properties are shown in Clause C.1.

7.3.3.2 Requirements

The safety case shall demonstrate the appropriateness in relation to the safety integrity level of the process, and the nature of the safety related process, of the following:

- the value of the time increment;
- the accuracy of the time increment;
- the size of the timer;
- the absolute value of the timer (e.g. UTC (universal coordinated time) or any other global clock);
- the synchronism of the timers in the various entities;
- the time delay between originating the information and adding a time stamp to it;
- the time delay between checking the time stamp and using the information.

7.3.4 Time-out

7.3.4.1 General

In transmission (typically cyclic) the receiver can check if the delay between two messages exceeds a predefined allowed maximum time (see Figure 2). If this is the case, an error shall be assumed.

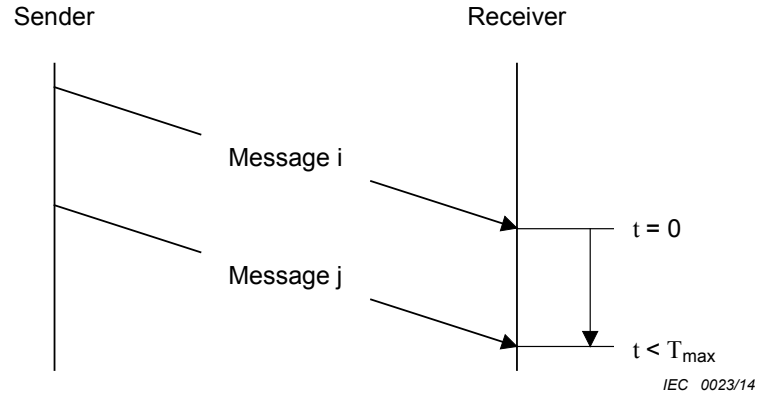


Figure 2 – Cyclic transmission of messages

If a return channel is available, supervision can be performed by the sender. The sender starts a timer when sending a message i. The receiver of message i responds with an acknowledge message j related to the received message i. If the sender does not receive the corresponding acknowledge message j within a predefined time, an error shall be assumed (see Figure 3).

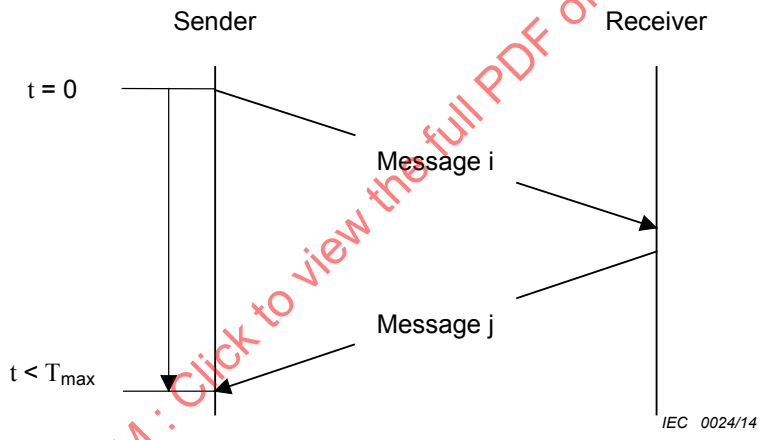


Figure 3 – Bi-directional transmission of messages

7.3.4.2 Requirements

The safety case shall demonstrate the appropriateness in relation to the safety integrity level of the process and the nature of the safety related process of the following:

- the acceptable delay;
- the accuracy of the time-out.

7.3.5 Source and destination identifiers

7.3.5.1 General

Multi-party communication processes need adequate means for checking the source of all information received, before it is used. Messages shall include additional data to permit this.

Messages may contain a unique source identifier, or a unique destination identifier, or both. The choice is made according to the safety related application. These identifiers are added in the safety related transmission functions for the application.

- Inclusion of a source identifier in messages can enable users of the messages to verify that messages are from the intended source, without the need for any dialogue between receiver and sender. This can be useful, for example, in unidirectional or broadcast communications.
- Inclusion of a destination identifier in messages can enable users of the messages to verify that messages are intended for them, without the need for any dialogue between receiver and sender. This can be useful, for example, in unidirectional or broadcast communications. Destination identifiers can be chosen to identify individual destinations, or groups of users.

7.3.5.2 Requirements

The safety case shall demonstrate the appropriateness, in relation to the safety integrity level of the process and the nature of the safety related process, of the following:

- the uniqueness of the identifiers for entities in the entire transmission system;
- the size of the identifier data field.

7.3.6 Feedback message

7.3.6.1 General

Where an appropriate return transmission channel is available, a feedback message may be sent from the receiver of safety-critical information to the sender. The contents of this feedback message may include

- data derived from the contents of the original message, in identical or altered form,
- data added by the receiver, derived from its own local information,
- additional data for safety or security purposes.

The use of such a feedback message can contribute to the safety of the process in a variety of ways:

- by providing positive confirmation of reception of valid and timely messages;
- by providing positive confirmation of reception of corrupted messages, to enable appropriate action to be taken;
- by confirming the identity of the receiving equipment;
- by facilitating synchronisation of clocks in sending and receiving equipment;
- by facilitating dynamic checking procedures between parties.

7.3.6.2 Requirements

The existence of a return channel does not intrinsically provide a defence against any identified threat; it is an enabling mechanism for other defences at the application level. Therefore, there are no specific safety requirements for such a feedback channel.

7.3.7 Identification procedure

7.3.7.1 General

The previous subclause covered the requirements for entities to be identified.

Open transmission systems can additionally introduce the risk of messages from other (unknown) users being confused with information originating from an intended source (a form of masquerade).

A suitably designed identification procedure within the safety related process can provide a defence against this threat.

Two types of identification procedure can be distinguished.

- Bi-directional identification
  Where a return communication channel is available, exchange of entity identifiers between senders and receivers of information can provide additional assurance that the communication is actually between the intended parties.
- Dynamic identification procedures
  Dynamic exchange of information between senders and receivers, including transformation and feedback of received information to the sender, can provide assurance that the communicating parties not only claim to possess the correct identity, but also behave in the manner expected. This type of dynamic identification procedure can be used to preface the transmission of information between communicating safety related processes and/or it can be used during the information transmission itself.

7.3.7.2 Requirements

Identification procedure forms a part of the safety related application process. The detailed requirements shall be defined in the safety requirement specification.

7.3.8 Safety code

7.3.8.1 General

In transmission systems, in general, transmission codes are used to detect random and/or burst errors, and/or to improve the transmission quality by error-correction techniques. Even though these transmission codes can be very efficient, they can fail because of hardware faults, external influences or systematic errors.

The safety related process shall not trust those transmission codes from the point of view of safety. Therefore a safety code under the control of the safety related process is required additionally to detect message corruption.

The safety case shall demonstrate the appropriateness, in relation to the required safety integrity and the nature of the safety related functions, of the following:

- the capability for detection of expected systematic types of message corruption;
- the probability of detection of random types of message corruption.

NOTE The safety code can be a combination of different codes, e.g. a linear code combined with a constant value.

Guidance for selection of safety codes is given in Clause C.3.

7.3.8.2 Requirements

7.3.8.2.1 The safety code shall be different from the transmission code, unless the message integrity is ensured by the safety code solely. This difference can be gained

- either by using different algorithms, or
- by using different configuration parameters (e.g. polynomials) for the same algorithms. If both codes are based on a CRC, the polynomials shall be different. If both polynomials have common factors, their contribution to the performance of the safety code shall be neglected in the safety analysis.

In the case of a closed transmission system, the designer can simply choose a safety code which is different to the transmission code, because he has full knowledge about the transmission system. In the case of an open transmission system, this requirement can be fulfilled by using a safety code which is not used by commercial transmission systems.

7.3.8.2.2 The safety code shall detect

- transmission errors, e.g. caused by EMI,
- systematic errors caused by hardware failures within the non-trusted transmission system.

Failures which would mimic the safety code cannot adequately be detected. Therefore the safety code has to be more complex than the expected failures. Hence it can be assumed that a hardware failure in the non-trusted transmission system cannot generate a valid safety code.

7.3.8.2.3 To fulfil the required safety integrity it is necessary that the safety code is sufficiently complex, e.g. based on a CRC, to detect and act on typical faults and errors. The analysis shall at least include:

- interrupted transmission line;
- all bits logical 0;
- all bits logical 1;
- message inversion;
- synchronisation slip (in case of serial transmission);
- random errors;
- burst errors;
- systematic errors, e.g. repeated error patterns;
- combinations of the above.

7.3.8.2.4 The probabilistic analysis of the performance of the safety code shall be compatible with the safety target. A model of the failure modes shall be provided and all assumptions made for the calculations shall be verified and validated.

The probability of undetected errors of linear codes is often calculated by using the binary symmetric channel (BSC) model (see Clause C.4). In the case the non-binary code is used, the q-nary symmetrical channel (QSC) can be more suitable. This standard recommends limiting this probability to the worst case value calculated by these models.

The BSC is well suited for random errors as caused by EMI. But simple random errors are usually eliminated by the non-trusted transmission system. Therefore, if an error is detected by the safety code, usually many bits in the safety related message are disturbed. Because no simple models are available for these cases, this standard recommends not using lower probabilities of undetected errors than the worst case value achieved by the application of the BSC for bit error rate less than one half (see Clause C.4).

An example of a simplified model for a closed transmission system is given in Clause C.4 (informative).

7.3.9 Cryptographic techniques

7.3.9.1 General

Cryptographic techniques can be used if malicious attacks within the open transmission network cannot be ruled out.

This is usually the case when safety related communication uses

- a public network,
- a radio transmission system,
- a transmission system with connections to public networks.

Against intentional attacks by means of messages to safety related applications, the safety related messages shall be protected with cryptographic techniques.

This requirement, aimed at avoiding masquerade from unauthorized senders, can be met by one of the following solutions:

a) use a safety code able to provide cryptographic protection;

b) encipher the messages after the safety code has been applied;

c) add a cryptographic code to the safety code.

These techniques can be combined with the safety encoding mechanism or provided separately. Annex C shows some possible solutions.

Cryptographic techniques imply the use of keys and algorithms. The degree of effectiveness depends on the strength of the algorithms and the secrecy of the keys. The secrecy of a key depends on its length and its management.

7.3.9.2 Requirements

The safety case shall demonstrate the appropriateness, in relation to the safety integrity level of the process and the nature of the safety related process, of the following:

- technical choice of cryptographic techniques, including
  - performance of encryption algorithm (e.g. symmetric or asymmetric),
  - key characteristics (e.g. fixed or session-based),
  - justification of selected key length,
  - frequency of key update,
  - physical storage of keys,
- technical choice of cryptographic architectures, including
  - checking the correct functioning (before and during the operational phase) of the cryptographic processes when they are implemented outside the safety related equipment,
- management activities, including
  - production, storage, distribution and revocation of confidential keys,
  - management of equipment,
  - review process of adequacy of cryptographic techniques, in relation to risks of malicious attacks.

The cryptographic algorithm shall be applied to all user data and may be applied over additional data that is not transmitted but is known to the sender and receiver (implicit data).

Reasonable assumptions shall be described about the nature, motivation, financial and technical means of a potential attacker, taking into account also developments (both technical, as in an increase in the power of computers, a decrease in the cost of fast processors, the spread of knowledge about algorithms, and ”social”, as in economic conflicts, a worsening of vandalism, etc.) that can be expected during the life-time of the system.

For key management, standardised techniques are highly recommended (e.g. according to ISO/IEC 11770 series).

7.4 Applicability of defences

7.4.1 General

The defences outlined in 7.3 can be related to the set of possible threats defined in Clause 5. Each defence can provide protection against one or more threats to the transmission. In the safety case it shall be demonstrated that there is at least one corresponding defence or combination of defences for each defined possible threat.

7.4.2 Threats/defences matrix

The Xs in Table 1 indicate that a defence can provide protection against the corresponding threat. The defences in Table 1 can be expanded in accordance with 7.2.7.

Table 1 – Threats/defences matrix

Threats	Defences							
	Sequence number	**Time stamp**	**Time-out**	**Source and destination identifiers**	**Feed-back message**	**Identification procedure**	**Safety code**	**Cryptographic techniques**
Repetition	X	X						
Deletion	X							
Insertion	X			X [a]	X [b]	X [b]		
Re-sequence	X	X						
Corruption							X [c]	X
Delay		X	X					
Masquerade					X [b]	X [b]		X [c]

[a] Only applicable for source identifier.
Will only detect insertion from invalid source.
If unique identifiers cannot be determined because of unknown users, a cryptographic technique shall be used, see 7.3.9.

[b] Application dependent.

[c] See 7.4.3 and Clause C.2.

7.4.3 Choice and use of safety code and cryptographic techniques

The choice of safety code and cryptographic techniques shall be determined according to the following:

- whether or not unauthorised access can be ruled out;
- the type of cryptographic code proposed;
- whether or not the safety related access protection process is separated from the safety related process.

Guidance on these issues is given in Clause C.2.

Annex A
(informative)

Threats on open transmission systems

A.1 System view

The threats to messages sent over the link by the control and protection system occur as a result of the possible changes in performance of the link, which can arise either in normal conditions (i.e. without failures) or abnormal conditions (i.e. following failures of the transmission system).

The adopted approach for deriving a set of threats has been that of splitting the hazard analysis, performed in form of a tree (see Figure A.1), into three separate levels:

- the user level;
- the network level;
- the external environment level.

These levels follow a top-down approach, starting from the main hazard (MH), which is the failure to obtain a valid message in terms of authenticity, integrity, sequence and timeliness at the receiving end.

Through the analysis of the possible message behaviours observed at the receiver part, the potentially dangerous situations (basic hazards) have been highlighted and a set of basic message errors (BME), intended as a classification of all possible message failure modes, has been outlined.

The derivation of the corresponding threats, to be understood as the network failure modes (i.e. the basic message errors seen from a network point of view), is straightforward. The threat is the entity that creates a dangerous situation for the safety (i.e. can lead to an accident) and is therefore a cause (at the network level) of a possible basic message error: the relationship threat-basic message error is consequently 1:1.

In its turn, a threat can be generated by a set of causes, called hazardous events (HE), which can be present at both the network and the external environment level. The same hazardous event can obviously be related to different threats.

Splitting the analysis into different levels also provides the possibility of (at least) three levels of defences:

a) one at a system/user application level, dealing with system implementation independently from the transmission field; an example is deletion, that can be non-dangerous if the system has been designed so that deleted messages do not represent a hazard;

b) one regarding the message logical structure; for example all the possible codes that can be applied to the message, or specific countermeasures such as sequence numbers, time stamps, etc.;

c) one at a physical level; an example is shielding to avoid corruption due to electromagnetic interference.

This annex will not deal further with this topic, which has been mentioned only with the aim of supplying an overall picture of the adopted methodology.

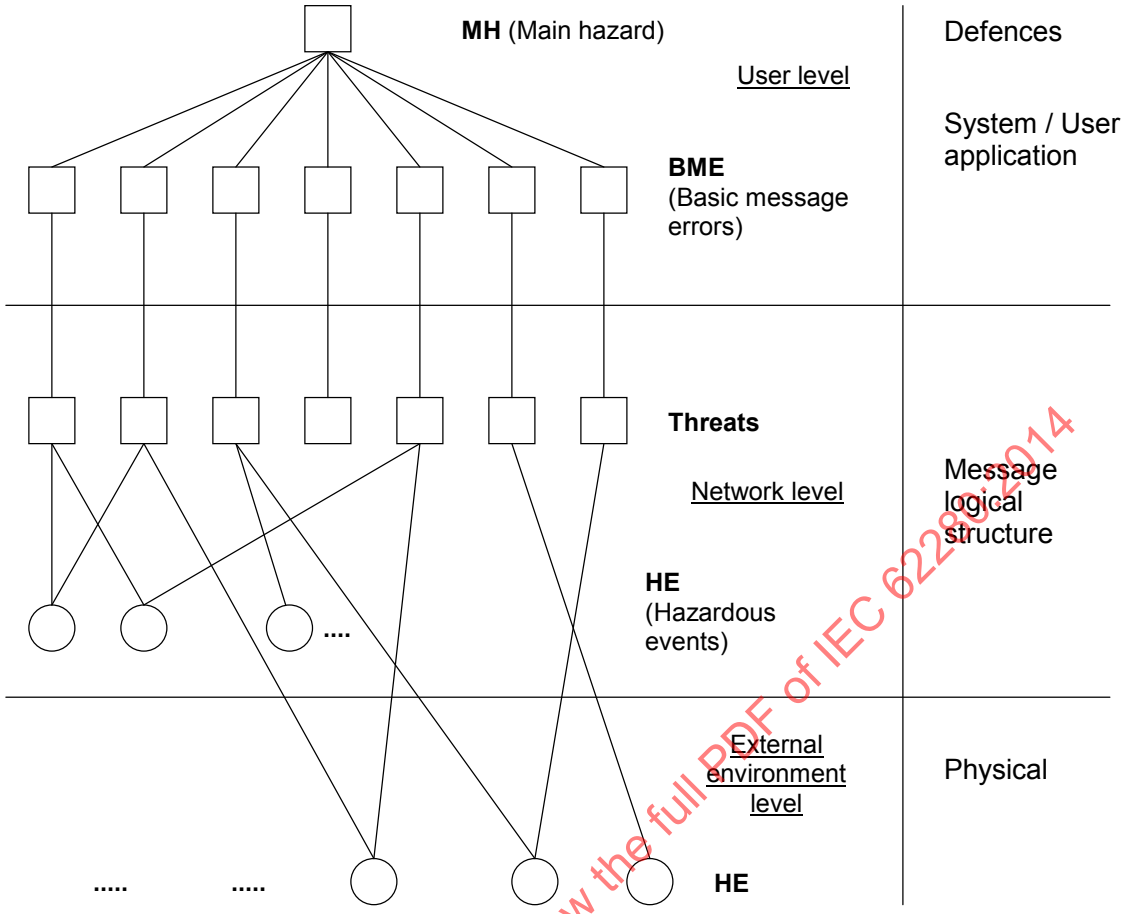


Figure A.1 – Hazard tree

A.2 Derivation of the basic message errors

The message is the main subject of the whole analysis, so the communication process has been studied from the point of view of the receiver. A message can be defined as “useful information originated by a source to be delivered within a time Δt from the beginning of the transmission”.

The integrity of the message stream is the main consideration in identifying the hazards that can occur in transmitting a safety related message over an open transmission system.

A “message stream” is defined as an ordered set of messages, and is unique for each time window and receiver in a network if no failures, attacks or incorrect operations occur.

The message stream actually received can be different from the expected one for a number of reasons. Three particular subclasses are specified (basic hazards):

- more messages received than expected;
- fewer messages received than expected;
- same number of received and expected messages.

More messages received than expected

In this case one or more messages have been repeated, or an external message has been inserted on the line. The basic message errors are therefore repeated, inserted message.

Fewer messages received than expected

In this case one or more messages have been deleted. The basic message error is therefore deleted message.

Same number of received and expected messages

In this case several possibilities can occur:

- all the messages in the stream are correct in content and in transit time but the sequence is wrong: re-sequencing has taken place;
- for a message in the stream it took longer than nominal Δt to reach the receiver: delay has taken place;
- the message has been modified: corruption has taken place;
- the receiver believes that the sender of a message is different from the real one: masquerade has taken place.

In the last two sub-cases, the integrity of the single message has been considered. The basic message errors are re-sequenced, delayed, corrupted, masqueraded message.

The following set of basic message errors has therefore been identified:

- repeated message;
- deleted message;
- inserted message;
- re-sequenced message;
- corrupted message;
- delayed message;
- masqueraded message.

The above defined basic message errors are not mutually exclusive: it is possible that more messages in a stream and even a single message are affected by more than one error mode.

A.3 Threats

A.3.1 General

Being the basic message errors the ones specified in Clause A.2, the derivation of the corresponding threats is straightforward.

Let A, B and C be three authorised parties that communicate safety related messages, while X is the attacker.

It has to be noted that also random and systematic HW/SW failures are taken into account in the list of threats; the following explanations are only examples and are therefore not exhaustive.

A.3.2 Repetition

– X copies a message [Maximum speed: 250 km/h] and replays it in an inappropriate situation [while train is in a slow speed track section],

or

– owing to a hardware failure the non-safe transmission system repeats an old message.

A.3.3 Deletion

– X deletes a message [X deletes the message Emergency Stop or Maximum speed: 250 km/h],

or

– a message is deleted due to a hardware failure.

A.3.4 Insertion

– X inserts a message [Maximum speed: 250 km/h],

or

– an authorised third party C involuntarily inserts a message in between the information flow from A to B (or the same happens due to a network error).

A.3.5 Re-sequencing

– X intentionally changes the sequence of messages for B (e.g. by delaying a message or by forcing the message to take a different path through the network),

or

– due to a hardware failure the message sequence is changed.

A.3.6 Corruption

– The message is accidentally changed (e.g. EMI) to another formally correct message,

or

– X alters a message [Maximum speed: 30 km/h to Maximum speed: 250 km/h] in a plausible way so that A and/or B cannot detect the modification.

A.3.7 Delay

– The transmission system is overloaded by the normal traffic (e.g. because of wrong design or an accidentally high amount of traffic),

or

– X creates an overload on the transmission system by generating bogus messages so that the service is delayed or stopped.

A.3.8 Masquerade

– A and B communicate safety related data,

and

– X pretends towards A to be B or towards B to be A (or both) to get access to the safety related data or to be regarded as a legal user of the system.

A.4 Possible approach for building a safety case

A.4.1 General

The approach that will be outlined hereafter is an example and is not the only one that can be followed. A complete hazard analysis needs in depth knowledge of the application to which it is related, in order to perform a proper risk assessment.

A.4.2 Structured methods for hazardous events identification

A.4.2.1 General

In the following, the analysis starts from the consideration that the examined case is dealing with a network interacting with the external environment. These two entities are structured in sub-entities (underlined in Figure A.2) that can be considered as the causes of the possible hazardous events to the analysed system. The network entity is subdivided according to the several steps of its life-cycle, while the splitting of the external environment entity takes care of its two possible characteristics: the physical and the human ones.

The leaves of the tree in Figure A.2 represent the causes of hazards: for each cause the corresponding generated hazardous events are identified. This way of proceeding also makes it easier, once the probability of a single cause is defined, to allocate the probability for each hazardous event produced.

In the following each cause is split into a number of possible hazardous events; this splitting is not exhaustive: during the hazard analysis some other hazardous events might be taken into account depending on the specific application.

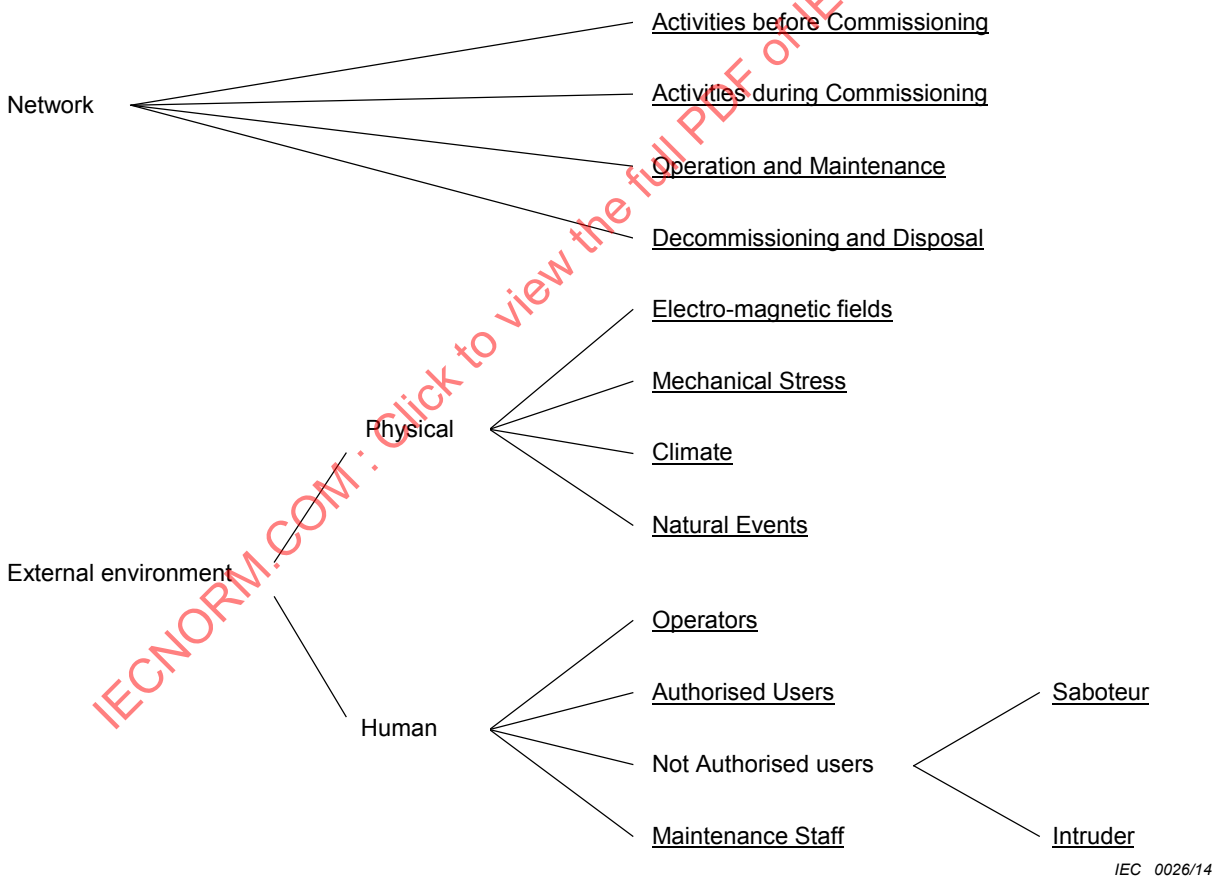


Figure A.2 – Causes of threats

A.4.2.2 Network

A.4.2.2.1 General

The phases of network life-cycle can be defined according to IEC 62278. For the scope of this annex (i.e. identification of hazardous events arising from “errors” in each phase), they can be grouped together in the following way:

- concept, system definition and application condition, risk analysis, system requirements, apportionment of system requirements, design and implementation, manufacture: all these phases are related to activities before the commissioning of the system;
- installation, system validation and system acceptance: these are related to the commissioning of the system;
- operation and maintenance;
- decommissioning and disposal.

A.4.2.2.2 Activities before commissioning

Errors during this phase can lead to

- HW systematic failure,
- SW systematic failure.

A.4.2.2.3 Activities during commissioning

Errors during this phase can lead to

- cross-talk,
- wires breaking,
- antenna misalignment,
- cabling errors.

A.4.2.2.4 Operation and maintenance

During this phase of life hazardous events can arise both from loss of performance of system components and from errors during repair and/or modifications:

- loss of performance;
- HW random failure;
- HW ageing.

A.4.2.2.5 Maintenance

- use of uncalibrated instruments;
- use of unsuitable instruments;
- incorrect HW replacement;
- incorrect SW upgrading or replacement.

A.4.2.2.6 Modification

- fading effects;
- human mistakes [1].

A.4.2.2.7 Decommissioning and disposal

It is not envisaged that hazardous events related to communication errors can arise during this phase of network life-cycle.

A.4.2.3 External environment

A.4.2.3.1 Electro-magnetic fields

- EMI;

---

[1] They depend on the particular type of application and cannot therefore be specified at this level of analysis.

- cross-talk (with external cabling or radio links).

A.4.2.3.2 Mechanical stress

- HW random failures;
- HW ageing.

A.4.2.3.3 Climate

- thermal noise;
- HW ageing;
- HW random failures;
- fading effects.

A.4.2.3.4 Natural events

- magnetic storm;
- fire;
- earthquake;
- lightning.

A.4.2.3.5 Operators

- Human mistakes [1].

A.4.2.3.6 Authorised users

- human mistakes [1];
- overloading of transmission system.

A.4.2.3.7 Maintenance staff

- use of uncalibrated instruments;
- use of unsuitable instruments;
- incorrect HW replacement;
- human mistakes [1];
- incorrect SW upgrading or replacement.

A.4.2.3.8 Saboteur [2]

- wire tapping;
- HW damage or breaking or changing;
- unauthorised SW modifications.

A.4.2.3.9 Intruder [2]

- monitoring of channels;
- transmission of unauthorised messages.

A.4.3 Relationship hazardous events – threats

Referring to Clause A.1, each threat can be seen as the set of hazardous events which generate it. Starting from the hazardous events identified in the previous subclause, the next step consists in building a relationship between them and the threats outlined in Clause A.3 by

---

[2] Both, saboteur and intruder are hackers, but the difference is that the first does not care what is on the line, his aim is only to modify the network, whilst the second does not alter the network, he utilises it in order to gain some advantage.

means of a bottom-up method [3]. The goal is to verify that no extra threat is found, in order to prove the validity of the approach undertaken. The relationship threats-hazardous events can be represented by Table A.1.

As can be seen, no extra threat has been discovered after analysing each hazardous event; this proves that the list of Clause A.3 is exhaustive.

(It has to be clear that the above table considers, for each hazardous event, only the primary effects, i.e. other relationships can be identified.)

A.5 Summary

Two different approaches for deriving the set of possible threats to safety related communication in transmission systems have been identified. The first one is a top-down method starting from the main hazard and ending with the classification of all the possible hazardous events leading to the hazard. The second one starts from the definition of the two main entities of the considered system (i.e. the network and the external environment) in order to classify all the possible causes of the hazardous events related to that system; these events are then referred to the threat(s) they generate.

The two analyses converge to the same set of threats, therefore both approaches can be used to analyse hazards on open transmission systems.

Table A.1 – Relationship between hazardous events and threats

Hazardous events	Threats						
	Repetition	Deletion	Insertion	Re-sequencing	Corruption	Delay	Masquerade
HW systematic failure	X	X	X	X	X	X	
SW systematic failure	X	X	X	X	X	X	
Cross-talk		X	X		X		
Wires breaking		X			X	X	
Antenna misalignment		X			X		
Cabling errors		X	X		X	X	
HW random failures	X	X	X	X	X	X	
HW ageing	X	X	X	X	X	X	
Use of uncalibrated instruments	X	X	X	X	X	X	
Use of unsuitable instruments	X	X	X	X	X	X	
Incorrect HW replacement	X	X	X	X	X	X	
Fading effects		X		X	X	X	
EMI		X			X		
Human mistakes	X	X	X	X	X	X	
Thermal noise		X			X		
Magnetic storm		X			X	X	
Fire		X			X	X	
Earthquake		X			X	X	
Lightning		X			X	X	
Overloading of TX system		X				X	

[3] Generally speaking, during the safety case analysis such a bottom-up method should be used to evaluate the threats which are caused by all the HE related to the particular application.

Hazardous events	Threats						
	Repetition	**Deletion**	**Insertion**	**Re-sequencing**	**Corruption**	**Delay**	**Masquerade**
Wire tapping	X	X	X	X	X	X	
HW damage or breaking		X			X	X	
Unauthorised SW modifications	X	X	X	X	X	X	X [a]
Transmission of unauthorised messages	X		X				X [a]
Monitoring of channels [b]							

[a] In this case the message is fraudulent from the beginning; a strong defence is needed, for example the use of a key.

[b] Unauthorised monitoring of SR messages is not considered to be a directly hazardous event; the hazard to system safety arises from “transmission of unauthorised messages” resulting from unauthorised monitoring. Confidentiality of application data is a separate system requirement outside the scope of this standard.

Annex B
(informative)

Categories of transmission systems

B.1 Categories of transmission systems

Subclause 6.3 identifies three categories of transmission system:

- Category 1 – Closed transmission systems, where all essential properties of the system are under the control of the safety related system designer, and a simplified set of safety requirements can be defined;
- Category 2 – Open transmission systems where, although the transmission is not fully under the control of the safety related system designer, the risk of malicious attack can be considered negligible;
- Category 3 – Open transmission systems where there is opportunity for malicious attack, and cryptographic defence measures are required.

The following Table B.1 gives some further guidance on how actual transmission systems that can be encountered in safety related applications may relate to the above three categories, on the basis of the characteristics of the technology they use, and key features of their configuration.

It is not possible to be precise about purely hypothetical example systems, but the main characteristics listed in the table may guide users of this standard towards determining whether a particular system should be regarded as a Category 1, 2 or 3 system for the purposes of analysis.

Table B.1 – Categories of transmission systems

Category	Main characteristics	Example transmission systems
Category 1	Designed for known and fixed maximum number of participants. All properties of the transmission system are known and invariable during the lifetime of the system. Negligible opportunity for unauthorised access.	Close air-gap transmission (e.g. track balise to train antenna). Proprietary serial bus internal to the safety related system (e.g. PROFIBUS, CAN, MVB (multi purpose vehicle bus defined by IEC)). Industry-standard LAN connecting different equipment (safety related and non-safety related) within a single system, subject to fulfilment and maintenance of the preconditions.
Category 2	Properties are unknown, partially unknown or variable during the lifetime of the system. Limited scope for extension of user group. Known user group or groups. Negligible opportunity for unauthorised access (networks are trusted). Occasional use of non-trusted networks.	Proprietary serial bus internal to the safety related system (e.g. PROFIBUS, MVB), but with the possibility that the transmission system could be reconfigured or substituted by another transmission system during the lifetime. Industry-standard LAN connecting different systems (safety related and non-safety related) within a controlled and limited area. WAN belonging to the railway, connecting different systems (safety related and non-safety related) at various locations. Switched circuit in public telephone network, used occasionally and at unpredictable times (e.g. dial-up remote diagnostic of an interlocking system). Leased permanent point-to-point circuit in public telephone network. Radio transmission system with restricted access (e.g. use of wave guides or leaky cables with a link budget limiting the possibility of reception to a close transceiver only, or using a proprietary scheme of modulation, impossible to reproduce with off the shelf or affordable lab equipment).
Category 3	Properties are unknown, partially unknown or variable during the lifetime of the system. Unknown multiple users groups. Significant opportunity for unauthorised access.	Packet switched data in public telephone network. Internet. Circuit switched data radio (e.g. GSM-R). Packet switched data radio (e.g. GPRS). Short range broadcast radio (e.g. Wi-Fi). Radio transmission systems without restrictions.

B.2 Relationship between the category of transmission systems and threats

The following Table B.2 shows a rough assignment of the threats to each of the categories of transmission systems defined above.

Table B.2 – Threat/category relationship

Category	Repetition	Deletion	Insertion	Re-sequence	Corruption	Delay	Masquerade
Cat. 1	+	+	+	+	++	+	-
Cat. 2	++	++	++	+	++	++	-
Cat. 3	++	++	++	++	++	++	++

Key

- \- Threat can be neglected.
- \+ Threat exists, but rare; weak countermeasures sufficient.
- ++ Threat exists; strong countermeasures required.

NOTE This matrix of threats is only a guide – analysis will always be necessary to determine whether countermeasures are required and to what degree. Each threat will be dependent on network type, application and configuration.

At this generic level, it is not possible to allocate SIL, according to the category of transmission system, to the defences needed for each threat; it is essential to analyse the particular application in order to allocate SIL.

Annex C
(informative)

Guideline for defences

C.1 Applications of time stamps

A time stamp can be used for different purposes.

a) To state the time of an event in an entity which is of importance for the process receiving the information. Events can be time related to each other. If we have knowledge of times and values for a sequence of events it is possible to interpolate between values and increase the accuracy of calculated values (e.g. for speed, acceleration). Transmission delays can be handled.

   Constraints:

   – if an absolute time stamp is used, the time in the entities needs to be synchronised. Each entity needs to have a safe time checking and update of the global time. The network delays have an effect on global clock distribution, information validity and process performance;

   – absence of messages will not be detected if a dialogue communication procedure is not provided.

b) To order event sequences which can be checked by the receiver.

   Constraints:

   – if the time granularity is too coarse, the sequencing properties of events can be indeterminate. In such cases the information should be complemented with sequence numbers;

   – the order of messages is affected by network routing of messages and time delays in the network;

   – absence of messages will not be detected if a dialogue communication procedure is not provided.

c) To measure time between events received from an entity sending a sequence of messages thereby also checking for events not being delayed.

   If information from an entity (A) is requested repeatedly from another entity (B), then the latter gets information of the partner's local clock from the time stamps. This information can be related to its own clock by taking the transfer delays into account. A logical clock has been created from the local clock of entity (B).

   Constraint:

   – the logical clock is affected by varying time delays in the network and the processing in entity (A).

d) To check the validity of information of an entity (A) by requiring a return of a time stamp delivered from an entity (B) in a previous message to the entity (A). This ensures a specific response (identity) and also checks against a predefined loop time. A sequence number (or label) created and time supervised in entity (B) will do the same work. No global time is needed (unless required by other applications).

   The receiver detects loss of information using a time-out.

Constraints:

– the procedure should handle interruption due to initialisation or fault conditions;

– the procedure will not guarantee authentication of the messages.

e) To create a procedure called double time stamping [UIC/ORE A155.1, see Bibliography]. This procedure inherits the properties of a combination of cases b), c) and d). The double time stamping procedure allows for asynchronous clocks in the entities thereby avoiding problems associated with keeping entities updated with global time. The method can be used for

– creating a logical clock from the partners' local clock and relative time stamps from the own local clock (and organising a clock synchronisation between the two entities),

– relating events to the relative time stamps including network delay,

– checking the correct order of messages,

– checking the partners' clock to verify the correctness of your own clock (application dependent).

The communication is valid for a two-partner dialogue or for a master-slave relation. The latter is more usable for cyclic transmission purposes rather than time-stamping single events where time is important for a special function.

Constraints:

– if the time granularity is too coarse, the sequencing properties of events can be indeterminate. In such cases the information should be complemented with sequence numbers;

– double time stamping could require knowledge about the round-trip transmission delays if the application considers case a) above.

More elaborated schemes than the double time stamps have been conceived which allow ordering events occurring on more than two systems [Tanenbaum].

C.2 Choice and use of safety codes and cryptographic techniques

Although the transmission system could be unknown or variable during its lifetime, in most cases one can determine whether malicious attacks to safety related messages can be excluded or not. This distinction is very useful because in case of the possibility of these malicious attacks, cryptographic mechanisms with secret keys are demanded. It is recommended to make this distinction at an early stage to limit the amount of safety related functionality. If there is the possibility of unauthorised access, a separate access protection layer can be applied (Type B0 or B1), see Figure C.1, or the protection is provided by the safety related transmission function using cryptographic mechanisms (Type A1) and in this case the term "cryptographic safety code" is used in the following text.

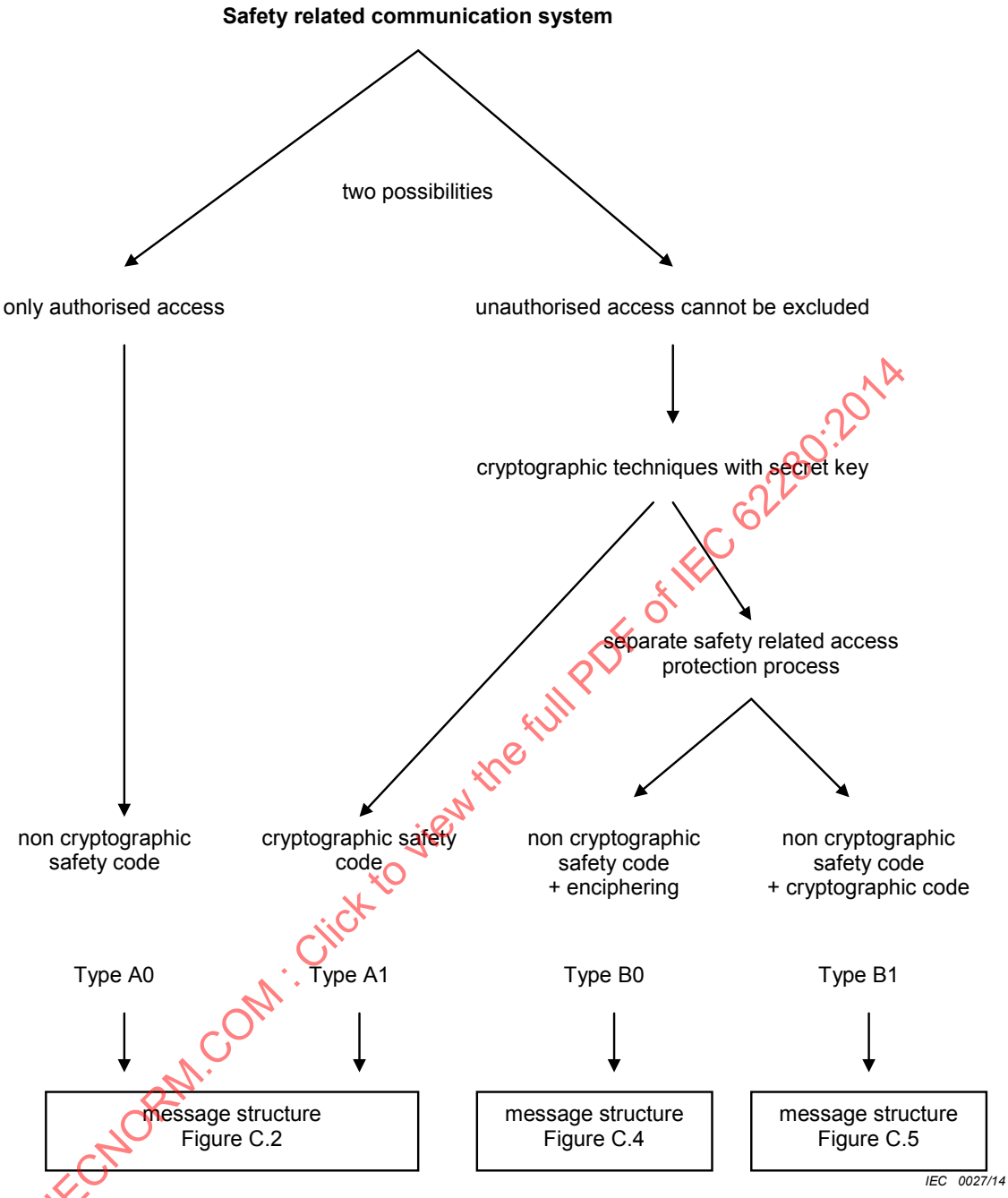


Figure C.1 – Classification of safety related communication systems

The principles of message structures for message Types A0 and A1 are depicted in Figure C.2.

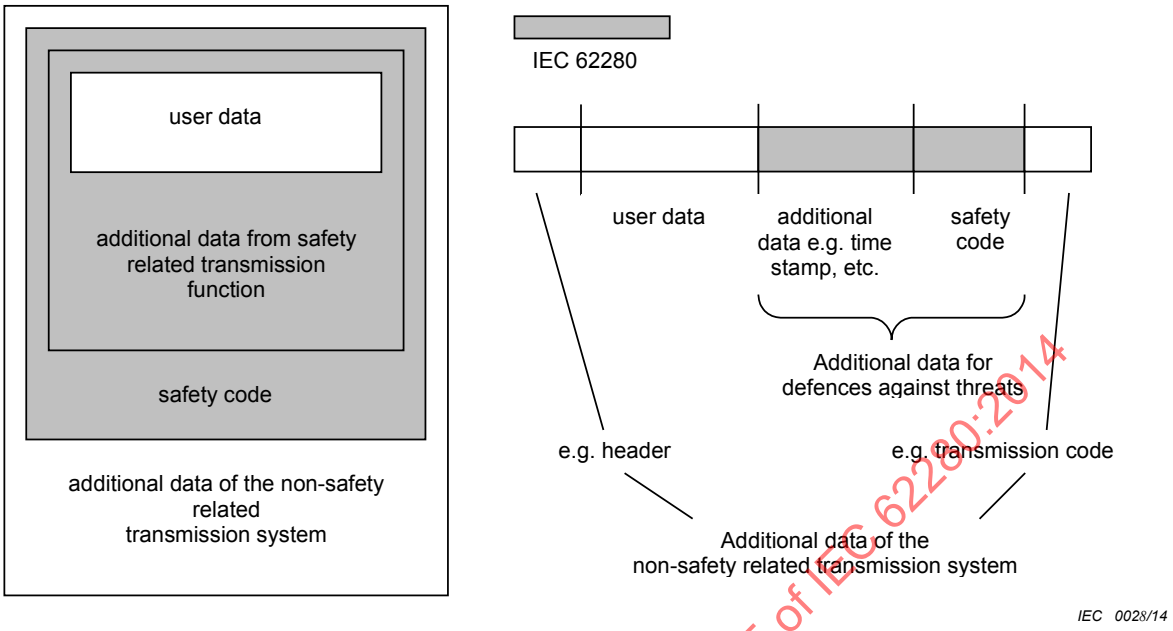


Figure C.2 – Model of message representation within the transmission system (Type A0, A1)

Separate access protection layers are useful, in those cases where groups of safety related computers which are connected by a local area network (LAN), have to communicate over open transmission systems (see Figure C.3). An implicit assumption behind the model depicted in Figure C.3 is that the LANs can be classified as Category 2. The cryptographic hardware and software can be concentrated at the unique entry point to the open transmission system. Other interfaces to the open transmission system should be excluded. The cryptographic functions can be combined with gateway functions which are normally required when a LAN is connected to a, for example, wide area network.

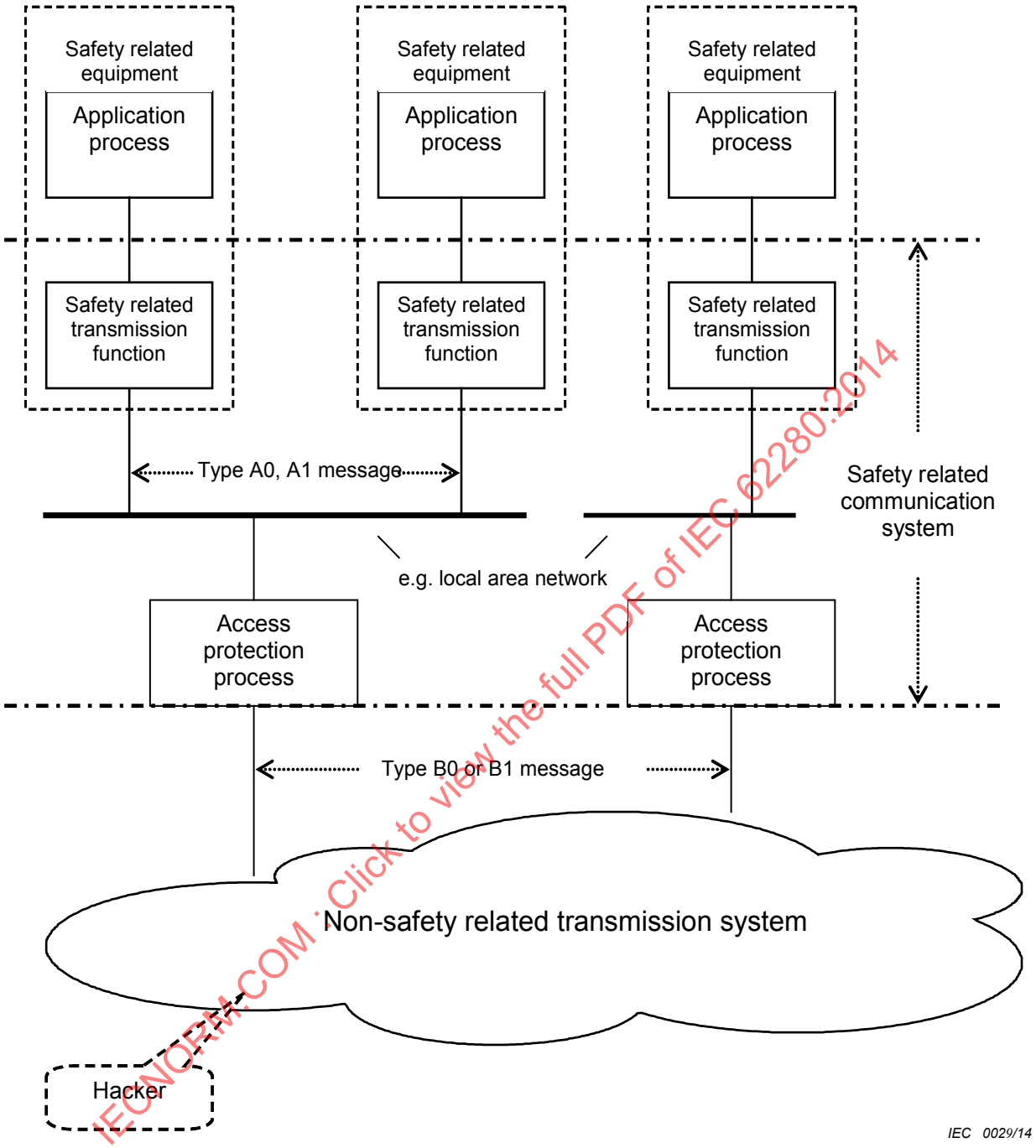


Figure C.3 – Use of a separate access protection layer

The access protection process can be performed by different modes:

a) enciphering of the messages;

b) adding a cryptographic code.

In both cases a safety code is applied before a safety related message is sent to the access protection layer. The equipment containing the access protection layer does not have to be safe by itself, see general requirements in 7.2. Note that failures of the access protection process should be considered.

The principles of message structures for message Types B0 and B1 are depicted in Figures C.4 and C.5.

These examples show the cryptographic protection being applied immediately after the safety code. In other examples it can be applied at lower levels (e.g. transport or network).

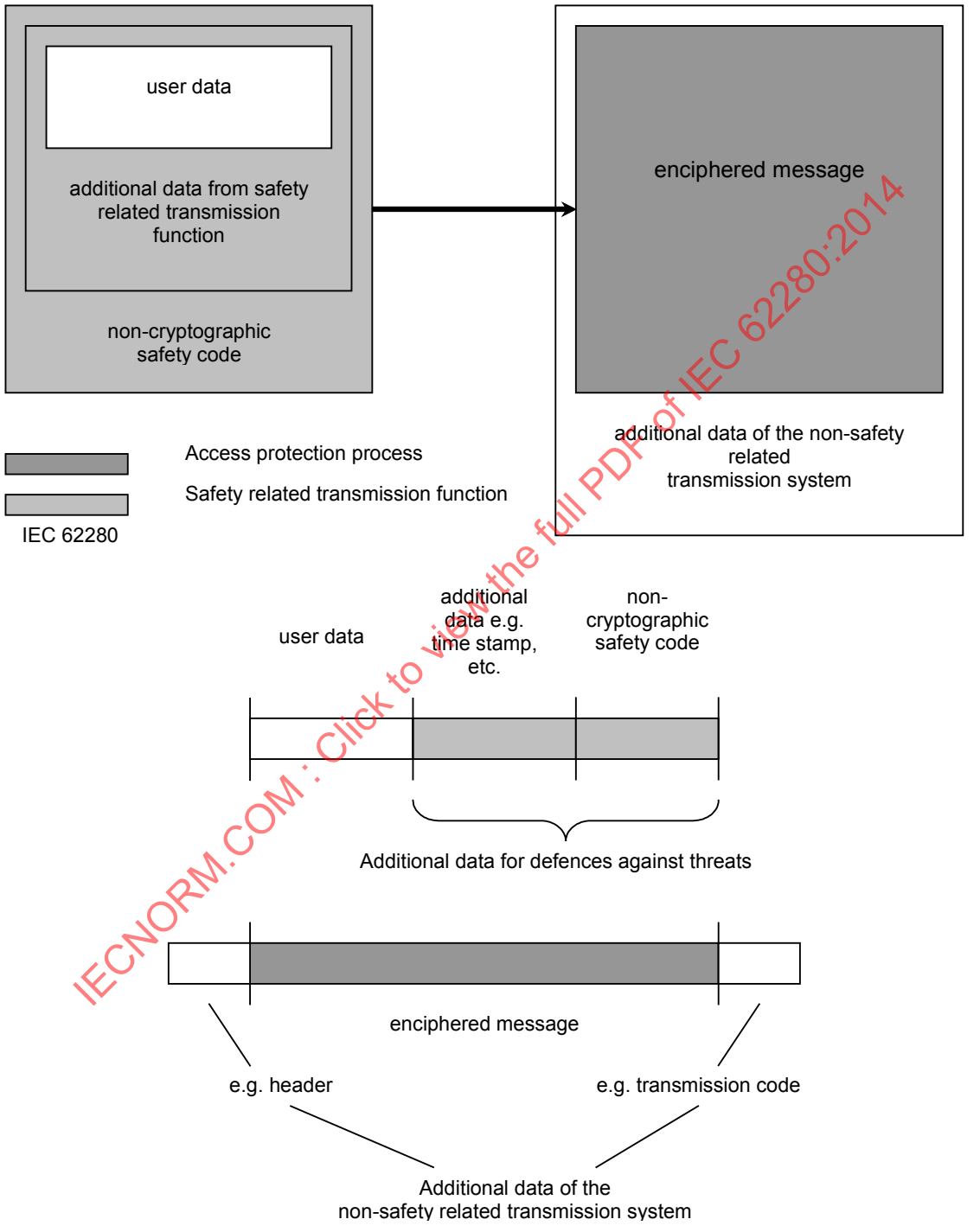


Figure C.4 – Model of message representation within the transmission system (Type B0)

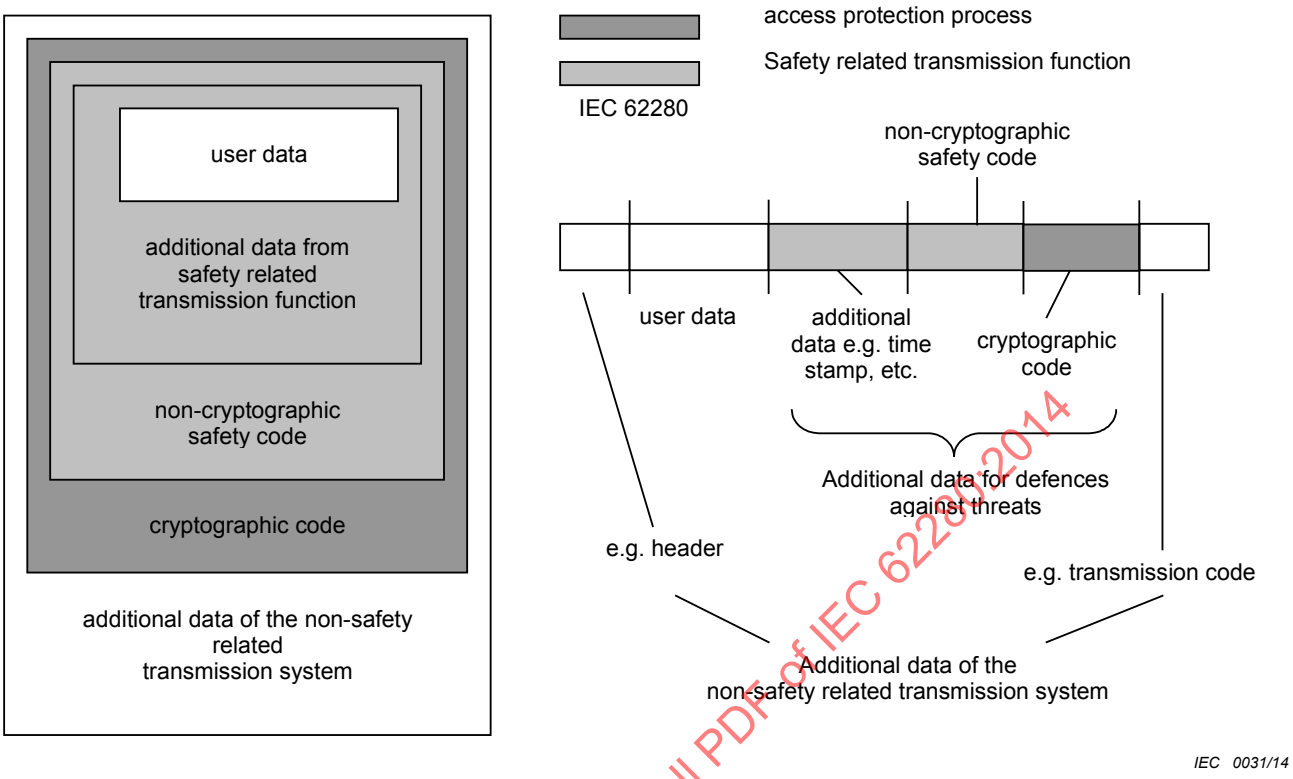


Figure C.5 – Model of message representation within the transmission system (Type B1)

C.3 Safety code

C.3.1 General

The required properties of the safety code depend on the characteristics of the transmission system and the architecture of the safety related communication system (see Figure C.1).

If unauthorised access to the transmission system can be excluded, the safety code has to detect all kinds of random and systematic bit errors. Note that usually the transmission system protects its messages with its own transmission code, which is already designed to meet a defined quality and bit error rate. Hence, if the transmission system delivers an invalid message, either the disturbance on the transmission channel was so great that the transmission code failed, or a failure has occurred. In either case, it should be considered that residual bit errors are not random, and can have any Hamming weight [Peterson].

If unauthorised access cannot be excluded, malicious attack cannot be prevented but can be detected and rendered harmless. The usual way to prevent a malicious attack is the application of cryptographic algorithms with at least one secret key. The safety code itself can be based on such an algorithm, or a separate access protection layer with cryptographic functions can be implemented. In the latter case, the safety code also can detect failures of the access protection equipment.

C.3.2 Main block codes

C.3.2.1 General

The following subclauses briefly describe some block codes and their main characteristics. See [Peterson] for more detail.

C.3.2.2 Linear block codes

A block code is linear if and only if the sum of any code words is also a code word.

Most of the codes in use for error control are linear binary codes. Non-binary codes are also used, e.g. Reed-Solomon codes. The codes are excellent for combating random errors and burst errors. The codes can be designed with a specific minimum Hamming distance *d*. That means that errors up to *d-1* wrong symbols are fully detected. Because of their linearity the codes can be tested for systematic transmission error detection capability.

The useful models are binary symmetric channel (BSC) and q-nary symmetric channel (QSC). The codes can also be tested for systematic transmission error detection.

C.3.2.3 Cyclic block codes

A linear block code is cyclic if every cyclic shift of a code word is also a code word. A cyclic code can be described by polynomials. The mathematics of codes can be found for example in [Peterson].

The codes are excellent for combating random errors and burst errors. The codes can be designed with a specific minimum Hamming distance *d*. The codes can also be tested for systematic error detection capability. A cyclic code with *c* redundant symbols detects all burst errors up to the length *c*.

In certain applications the cyclic nature of the code can be exploited to avoid the danger of false code word synchronisation. To achieve this it is necessary to extend the code but the end result will be superior to systems relying on separate synchronisation characters.

C.3.2.4 Hash block codes

Hash codes can be linear or non-linear. Most important are non-linear one-way functions, which compress input data to a “fingerprint”. Because of their non-linearity, a minimum Hamming distance cannot be derived except for trivial small cases. However, the error detection capability is high for good hash codes. A single bit change in the input data changes, on average, half of the bits in the hash value. Given a hash value, it is computationally unfeasible to find the input data that hash to that value (one-wayness property) and, given the input data, it is computationally unfeasible to find another input data that hash to the same value (collision property for weak hash functions) and it is computationally unfeasible to find any two sets of input data that hash to the same value (collision property for strong hash functions).

ISO/IEC 10118-1 defines in a general way hash-codes for security purposes. ISO/IEC 10118-2 describes hash-codes using an *n*-bit block cipher algorithm without applying a key. Also, a MAC can be used as a hash-code, but in this case a key is required.

Good performance in software can be obtained with the public domain message digest algorithms MD4 and MD5 [Rivest] which are classes of MDC. No high requirements on collisions' criteria are demanded because malicious attacks are defended by other means. That means that either a cryptographic block code (MAC) is used, or a cryptographic protection over the entire safety related message including the hash value is applied.

C.3.2.5 Digital signatures

A digital signature is a number of bits depending on all the bits of the input data (user data and additional data) and also on a secret key. Its correctness can be verified by using a public key [Davies].

C.3.2.6 Cryptographic block codes

Cryptographic block codes are a kind of non-linear hash block code based on cryptographic algorithms. The advantage is that they can protect against malicious attack if they are based on keys. The most well known code is the message authentication code MAC that is standardised in ISO/IEC 9797-1 and ISO/IEC 9797-2.

C.3.3 Recommendations for the application of safety codes

Examples for the assessment of diverse basic techniques are given in Table C.1.

Table C.1 – Assessment of the safety encoding mechanisms (see note)

Type [a]	Reference, see Clause 2 and Bibliography	Type of safety related communication system, see Figure C.1			
		A0	A1	B0 [b]	B1 [b]
CRC [c]	[Peterson]	R	US [d]	- [e]	R
MAC [c]	ISO/IEC 9797-1 and 2	R	HR	R	R
Hash code [c]	ISO/IEC 10118-2	R	US [d]	HR	HR
Digital signature [c]	ISO/IEC 9796-2 and 3	R	R	R	R

NOTE Where more than one safety encoding mechanism is recommended, an appropriate combination of one or several mechanisms should be selected.

HR	This symbol means that the technique is Highly Recommended for this architecture. If this technique is not used then the rationale behind not using it should be detailed in the technical safety report.
R	This symbol means that the technique is Recommended for this architecture. This is a lower level of recommendation than 'HR'.
-	This symbol means that the technique or measure has no recommendation for or against being used.
US	This symbol means that this technique is unsuitable as a defence in this category of system.

[a]	Other safety measures are possible but not considered here.
[b]	Non-cryptographic safety code only. Cryptographic techniques to be considered separately.
[c]	The error detection capability is similar for the same number of redundancy bits.
[d]	Secret key demanded, cannot be performed by this mechanism.
[e]	If stream ciphering techniques are used then applying a CRC as safety code is unsuitable. Otherwise, an attacker can create safety related messages with a valid CRC by adding an arbitrary message with a valid CRC to the stream ciphered message, without breaking the key.

Although knowledge of the error characteristics of a particular channel may enable some type of error to be disregarded, and better performance to be claimed, in an ”open” channel (black channel) no such knowledge can be assumed. In this scenario the ideal solution would be a random code. For this reason no claim for the probability of undetected error p_{UE} of a safety code should be made, which is lower than the performance of the random code, which is $p_{UE} = 2^{-c}$, where c denotes the number of redundancy bits.

C.3.4 Cryptographic techniques

When using ciphering techniques, standardised modes of operation are recommended, e.g. according to ISO/IEC 10116. This standard does not recommend the Electronic Codebook mode (ECB) for input lengths which exceed the block length of the enciphering algorithm.

Well-known and well-tested algorithms such as [FIPS PUB 197] are recommended.

C.4 Length of safety code

This annex is applicable for Category 1 only, i.e. closed transmission systems, since the given formulae are based on specific assumptions on the transmission system.

In fact the model described here relies partly on the error detecting and managing mechanisms of the transmission systems. Usually, under fault free conditions, the error detecting mechanism of the transmission system detects and counteracts all transmission errors. In this case the safety code will not detect any errors. Nevertheless, the transmission system itself or its error detecting mechanism can fail because of hardware failures, or some transmission errors are so high that they are not detected. In all these cases the safety code has to detect those failures.

Using this model leads to lower safety integrity requirements for the safety code in comparison to models neglecting the error detecting capabilities of the transmission system. On the other hand, the transmission system is now fixed and cannot be exchanged for another one without adapting the safety case. This model can be (and should be if necessary) modified for systems ignoring their error detecting mechanisms or the influences coming from the hardware failure rate.

This annex gives simple formulae for calculating the length of the safety code. Fulfilling the given requirements guarantees that the safety target will be reached.

The basic model for calculating the length of the safety code is shown in Figure C.6.

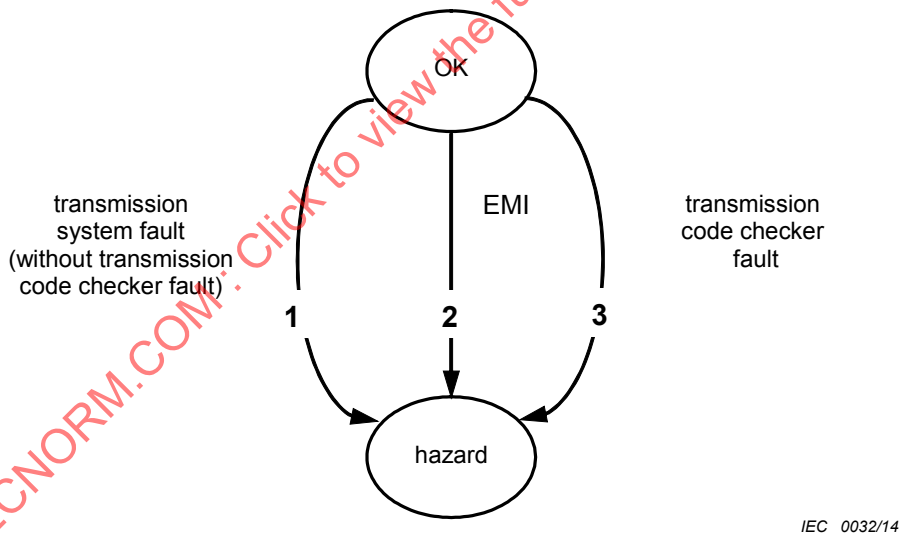


Figure C.6 – Basic error model

There are three ways in which a hazard can be created:

a) the transmission hardware fails, so the messages are corrupted;

b) bit errors arise due to EMI and are not detected by the transmission coding;

c) faults occur in the transmission code checker, such that every corrupted message could be passed from the non-trusted transmission system to the safety related equipment.

The following definitions are given:

R_{H} Target hazardous failure rate of the complete transmission system

R_{H1} Hazardous failure rate of hardware faults without transmission code checker

R_{H2} Hazardous failure rate of EMI

R_{H3} Hazardous failure rate of transmission code checker

R_{HW} Hardware failure rate of the non-trusted transmission system

p_{US} Probability of undetected failure due to the performance of the safety code

p_{UT} Probability of undetected failure due to the performance of the transmission code

NOTE 1 When the non-trusted transmission systems contain no transmission coding mechanisms then p_{UT} = 1 has to be assumed.

f_M Maximum frequency of messages for one receiver

f_W Frequency of wrong (corrupted) messages

T Time span, if more than a defined number of corrupted messages were received within this time, the safe fall back state will be entered

k_1 Factor for hardware faults including safety margin

k_2 Factor which describes the percentage of hardware faults that result in undetected disabling of transmission decoding

m Safety factor included within k_1

n Number of consecutive corrupted messages until the safe fall-back state is entered

With these definitions the following formulae have to be evaluated:

$$R_{HW} \times p_{US} \times k_1 = R_{H1} \quad \text{(C.1)}$$

$$p_{UT} \times p_{US} \times f_W = R_{H2}^{4} \quad \text{(C.2)}$$

$$k_2 \times p_{us} \times \frac{1}{T} = R_{H3} \quad \text{(C.3)}$$

The sum of all three rates should not exceed R_H:

$$R_{H1} + R_{H2} + R_{H3} \leq R_H$$

Because it cannot be assumed that the failure is random, it is necessary to take into account a safety margin m in the factor k_1. The factor k_1 should be calculated according to the following formula:

$$k_1 \geq n \times m$$

The factor m represents the safety margin with $m \geq 5$.

The maximum frequency of wrong messages f_W should be estimated

- either by the worst case estimation $f_W = f_M$,
- or by limiting the maximum rate or number of wrong messages where safe counters and/or safe timers are implemented. If more than one wrong message within a definite time interval is received, the safe communication should be aborted and the safe fall back state should be entered. A mathematical derivation proves that a certain limit cannot be exceeded.

4 This assumes that the safety code and the transmission code are independent. This can be very hard to prove. A more conservative approach is to rely only on the safety code.

In cyclic transmission the frequency f_M is well defined. In case of non-cyclic transmission the maximum possible frequency shall be taken.

By using proper or good CRC [5] the maximum value of p_{UT} may be estimated as

$$p_{UT} = 2^{-b}$$

where b denotes the number of redundancy bits.

If other codes are used, e.g. a combination of two codes, the worst case block error probability using the model of “binary symmetric channel" [6] should be taken.

The factor k_2 is difficult to estimate. If periodic checking of the correct working of the transmission encoding mechanism is possible, then the factor k_2 could be neglected.

Without any justifications $k_2 = 1$ should be taken.

NOTE 2 The following derivation is given for information only.

- If a hardware fault occurs, in only 1 of 10 000 cases the transmission code checker fails undetected.
- In this case the average duration (without EMI) of this state is

$$T = \mathrm{MTBF}_{HW} = \frac{1}{R_{HW}}$$

Note that a small degradation of transmission quality would usually lead to the safe fall back state, so this estimation is very pessimistic.

Under these assumptions the value $k_2 = 10^{-4}$ can be taken.

Formula (C.3) leads to a minimum time interval, in which only one error detected by the safety code is allowed. If such a mechanism is not used, the safe fall back state shall be entered immediately after the first detected error, otherwise other measures against possible error conditions shall be introduced.

The maximum probability for undetected errors of the safety code with c digits should be estimated as

$$p_{US} = 2^{-c}$$

This formula can be used as a rough estimation of the probability of undetected faults. This is valid for a large class of codes (e.g. Hamming codes, some BCH-codes, cryptographic codes, etc.) under realistic assumptions. Nevertheless, it has to be demonstrated that the properness or goodness [5] of the chosen linear code is fulfilled.

By repeating each message and checking the consistency of two mutually independent messages the value of c can be halved at least to reach the same target. In fact one can gain some further improvement, but in order to avoid intricate mathematical calculations the given pessimistic estimation should be the limit.

---

5 Properness means that the relation between bit error probability (less than one half) and probability of undetected error is monotone. Goodness means that the probability of undetected error has its absolute maximum at the bit error probability of one half. See e.g. Wolf, J. K., Michelson, A. M. und Levesque, A. H.: "On the probability of undetected error for linear block codes", IEEE COM-30, 1982, 317-324; Dodunekova R., Dodunekov S. M.: "Sufficient conditions for good and proper detecting codes", IEEE Trans. Inform. Theory, vol. 43. pp. 2023-2026, Nov. 1997.

6 Binary symmetric channel: With probability p a received bit is falsified (0→1 and 1→0). Each bit is independent from each other.

NOTE 3 This mechanism relies on the fact that common cause failures affecting the two messages are negligible.

C.5 Communication between safety related and non-safety related applications

An example of communication between non-safety related applications and safety related applications is shown in Figure C.7.

Within trusted networks (Category 1 and 2) non-safety related applications can communicate over the same transmission media used by safety related applications. For requirements therefore, see 7.2.

In this example the non-safety related message is also protected by cryptographic techniques when passing through a Category 3 transmission system.

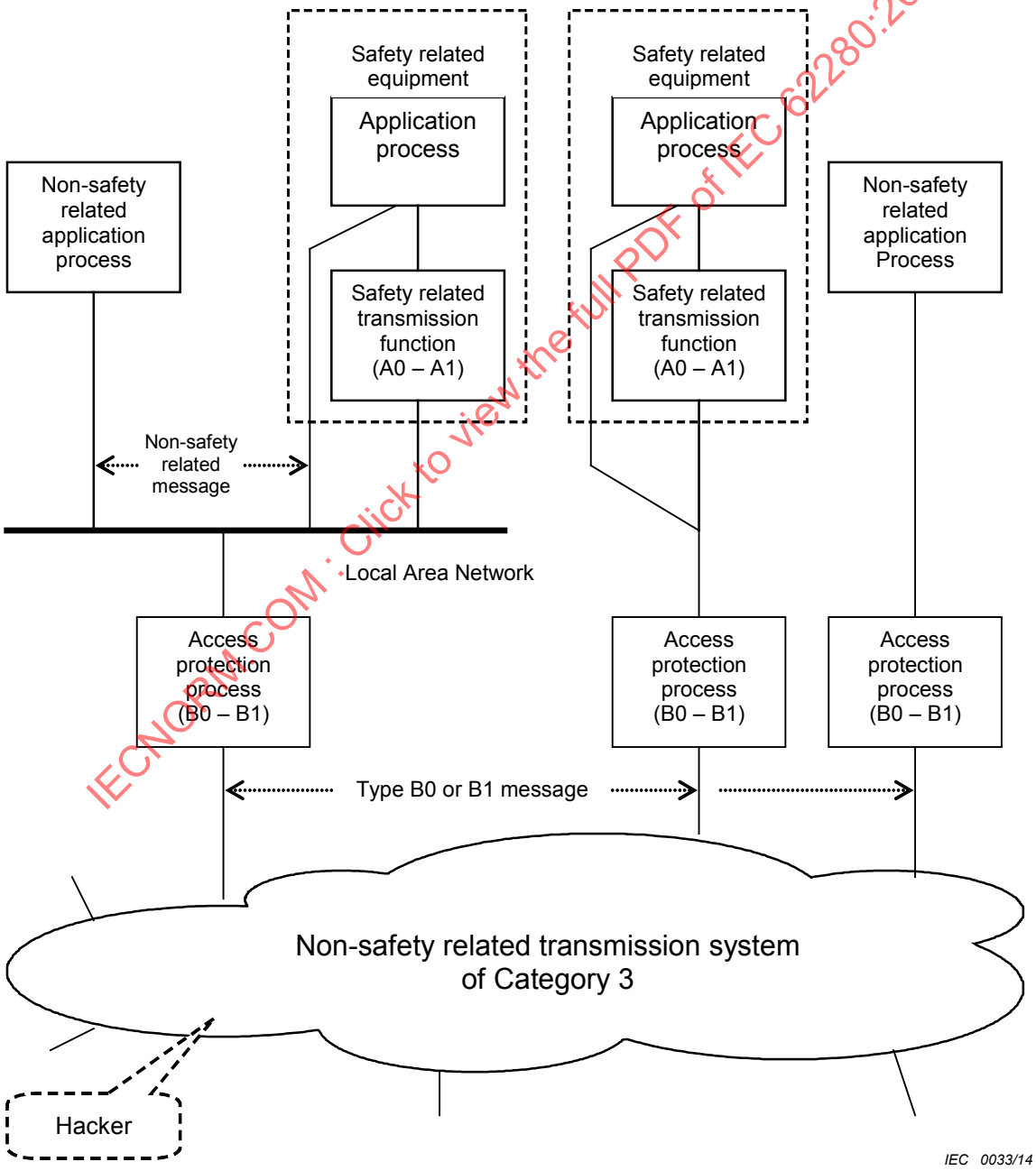


Figure C.7 – Communication between non-safety related and safety related applications

Annex D
(informative)

Guidelines for use of the standard

D.1 Procedure

D.1.1 General

A number of distinct steps can be identified to carry out the system design activities covered by IEC 62425.

These steps are identified below:

Application
↓
Hazard analysis
↓
Risk reduction
↓
Allocation of SIL and quantitative targets
↓
Safety requirements specifications (SRS)

Each of these steps is described in more details in the following subclauses.

D.1.2 Application

The system designer shall understand the application of the transmission system. The data flows, types of data, and the frequency and the nature of updates (e.g. periodic or event driven) all affect the decisions to be made in designing the transmission system. The global safety target (rate or qualitative parameters and non-functional parameters) for the system shall also be defined (by the user or the safety authority).

D.1.3 Hazard analysis

Qualitative hazard analysis of the system (as required by IEC 62278) shall identify the top-level hazard(s) which can arise as a result of failures of the sending and receiving equipment, or of the transmission link itself. This analysis shall consider operational or other external conditions which could expose the system to the hazard. For each threat to the system, the possibility of including a defence in the system design can be included.

D.1.4 Risk reduction

From the global quantitative safety target for the system, and the qualitative hazard analysis, the system designer can apportion safety targets to each threat identified. The allocation of such targets may be iterative, beginning from a simplistic allocation, and refined in accordance with more detailed analysis and trade-off between cases. Using quantitative information about the occurrence of external conditions exposing the system to hazard, the extent of risk reduction needed from each defence can be determined.

D.1.5 Allocation of SIL and quantitative targets

Depending on the extent of risk reduction needed for each defence, SIL can be allocated, using the procedures defined in IEC 62425. Knowing the SIL for the defence, appropriate design techniques can be selected, for use in work associated with that defence.

From the quantified unsafe (wrong-side) failure rate identified for the defence, hardware design techniques can be chosen using the tables in IEC 62425, and the rate of occurrence of unsafe failures due to random faults can be calculated.

D.1.6 Safety requirements specifications (SRS)

The defences identified as being necessary for safe operation of the system, the SIL for the implementation of those defences and quantified safety targets for the system shall be recorded in the SRS for the system.

D.2 Example

D.2.1 General

The following example shows only some basic principles of the procedure. It was not intended to describe a complete example which is correct in all details.

D.2.2 Application

Movement authority commands are sent to trains on a secondary line by means of messages over a radio network.

A global safety target of 10^{-x} per hour is defined for the system.

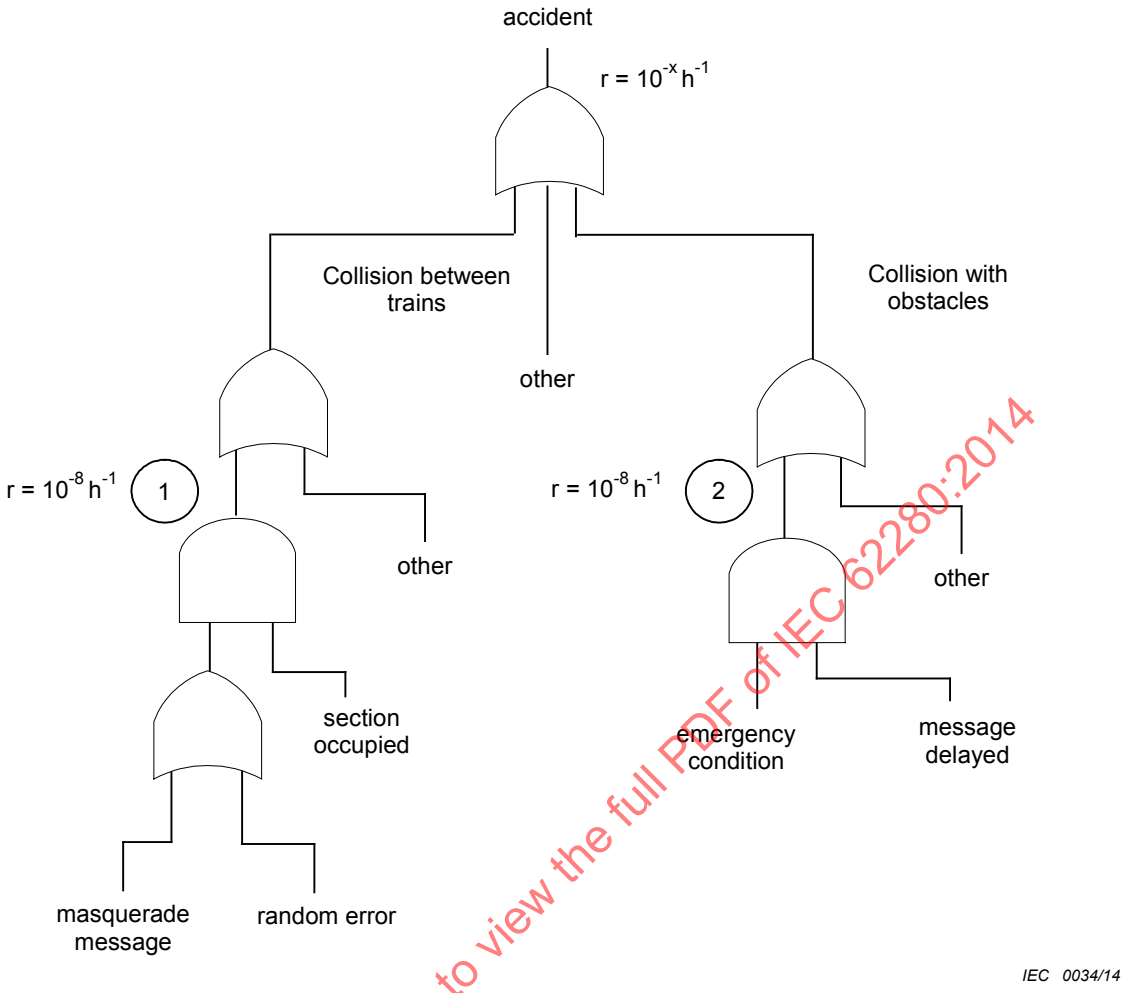
D.2.3 Hazard analysis

Two particular hazards can be identified (among others not considered here):

a) reception of an incorrect (wrong-side) message on-board a train could result in the train entering an occupied section, and colliding with another train;

b) delay in receiving an emergency stop message could result in a train colliding with an obstruction on the track.

These are shown on a fault tree (Figure D.1), as an example of one method of performing the hazard analysis.



Key

OR gate

AND gate

1 Fault tree for case 1 (see Figure D.2)

2 Fault tree for case 2 (see Figure D.3)

r Tolerable hazard rate

NOTE Preferred symbols according to IEC 61025.

Figure D.1 – Fault tree for the hazard "accident"

The 10^{-x} per hour global safety target for the system is apportioned, and the target allocated for cases 1 and 2 is (for example) 10^{-8} per hour in each case.

Cases 1 and 2 will be considered in detail.

D.2.4 Case 1

D.2.4.1 Risk reduction

If a message to a train is corrupted due to random errors, it can permit the train to enter an occupied section, and collide with another train.

In addition, deliberate attempts could be made to insert an incorrect message into the system (e.g. by a hacker).

Suppose the probability of the section being occupied is judged to be 10^{-1}.

This standard suggests that a possible defence against message corruption is to use a safety code attached to the user information in the message.

Introducing this defence into the portion of the fault tree for this case, the following Figure D.2 results:

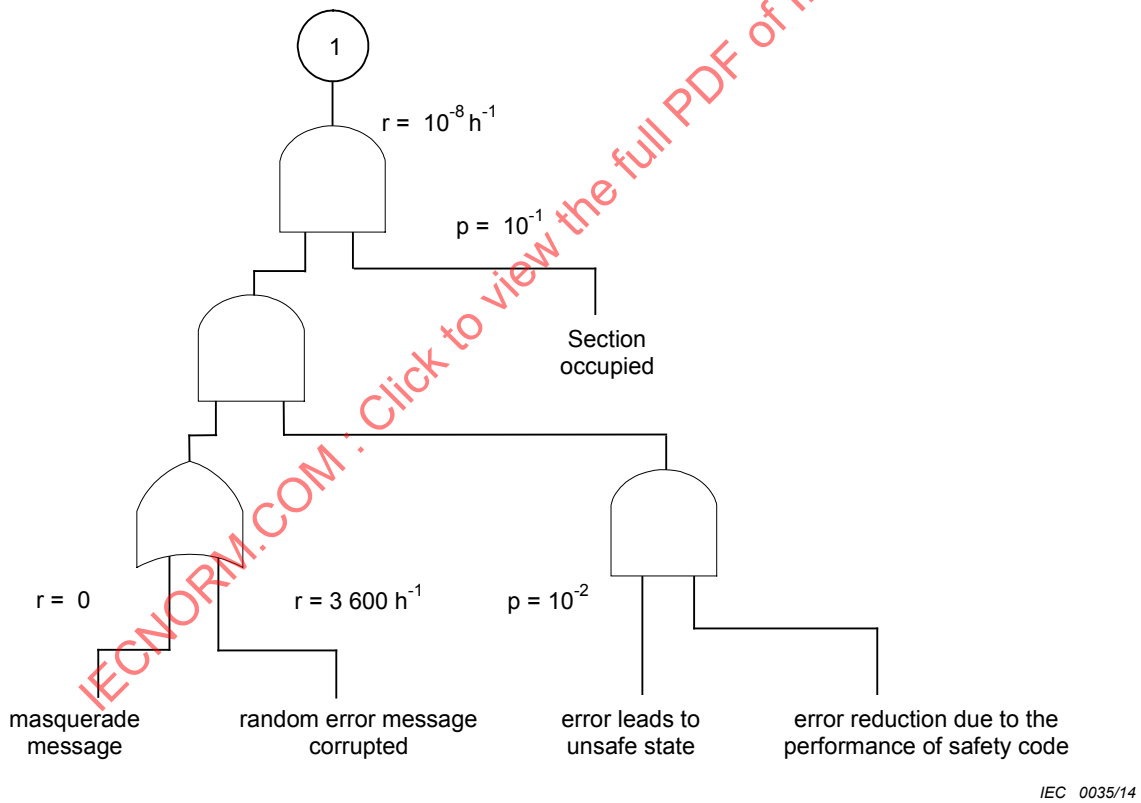


Figure D.2 – Fault tree for case 1

Considering quantitative safety targets, it shall be assumed that, in an open system, every message could be corrupted (i.e. probability = 1). However, not every corrupted message will authorise the train into the particular section. Assuming this probability is 10^{-2}, and assuming that a message with the length of 100 bits is sent to a train over a channel with the bit rate of 100 bits/s (i.e. 3 600 messages per hour), it is clear that the safety code for the message shall guarantee a probability of undetected error of less than 3×10^{-9} per message, or the frequency of this kind of events should not exceed 10^{-5} h^{-1}.

D.2.4.2 SIL allocation and quantified target

According to IEC 62425 a SIL for the implementation of the function “computing of safety code” can be derived. This SIL could be lower than for the entire system element “safety related communication system”.

The designer of the system shall select a safety code with a sufficient length to achieve the required performance.

This standard suggests that it is necessary to consider the possibility of deliberate attempts to create incorrect messages in an open transmission system. For example, for infrequent transmission of short messages, the likelihood of deliberate attempts to create accidents could be relatively low. These factors may influence the decision on whether to adopt a cryptographic safety code, and if so, on the choice of parameters (key length, etc.) for this code.

D.2.5 Case 2

D.2.5.1 Risk reduction

If, when an emergency condition (e.g. obstruction on the track) occurs, the emergency stop message to the train is delayed a collision could result. Suppose that such emergency conditions are judged to occur with a frequency of 10^{-4} per hour.

Suppose that, using a radio network shared with an uncontrolled number of other users, no maximum message delay is guaranteed, and delay shall therefore be assumed (i.e. the delay is assumed to have a probability of 1).

This standard suggests that a possible defence against message delay is to use a time-out in the receiving equipment, together with cyclic message transmission.

Introducing this defence into the portion of the fault tree for this case, the following Figure D.3 results:

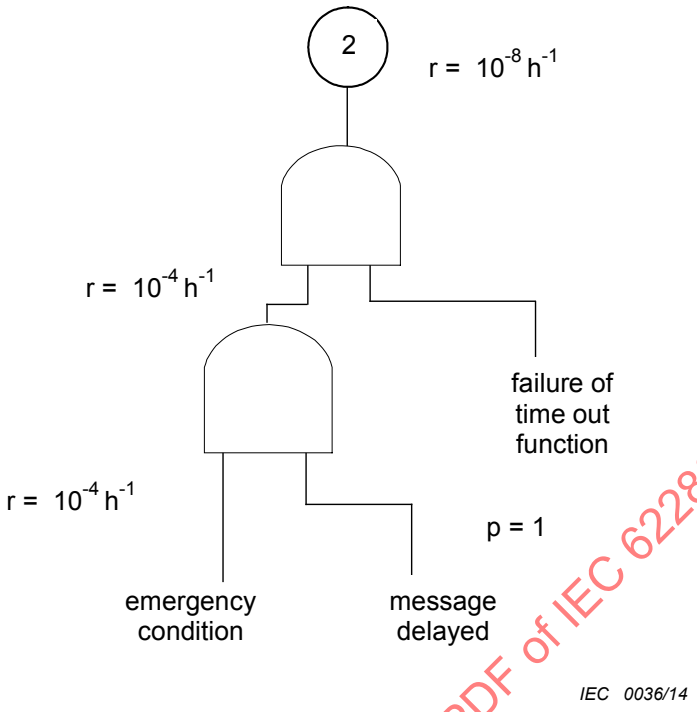


Figure D.3 – Fault tree for case 2

Considering quantitative safety targets, it is clear that the time-out shall have a wrong side error probability of not more than 10^{-4} on demand.

D.2.5.2 SIL allocation and quantified target

Reference to IEC 62425 indicates how to achieve the required SIL.

The implementation of this function shall therefore be designed using techniques suggested in IEC 62425 as being appropriate for derived SIL, unless the implementation is integrated with other functions with a higher SIL (e.g. in a processor system).

Annex E
(informative)

Mapping from previous standards

This International Standard is the result of revision and merging of the previous standards IEC 62280-1:2002 and IEC 62280-2:2002. Primarily only corrections and improvements were carried out. Some new parts were necessary due to consistency reasons.

Tables E.1 and E.2 show the mapping of the (sub)clauses and annexes of the previous standards IEC 62280-1(2002) and IEC 62280-2(2002) to the (sub)clauses and annexes of this standard IEC 62280.

These should facilitate the traceability in case of maintenance and/or extensions of systems once approved according to the previous standards IEC 62280-1(2002) and IEC 62280-2(2002) and furthermore the understanding of this standard IEC 62280.

The references in Tables E.1 and E.2 are only from the previous standards to the new standard, but not vice versa.

Table E.1 – Mapping from IEC 62280-1:2002 to IEC 62280

(Sub)clause of IEC 62280-1:2002		Informative / Normative	(Sub)clause of IEC 62280		Unchanged / Modified
Introduction		Inf.	Introduction		E
1	Scope	Nor.	1	Scope	E
2	Normative references	Nor.	2	Normative references	E
3	Definitions	Nor.	3	Terms, definitions and abbreviations	E
4	Reference architecture	Nor.	4	Reference architecture	T
	Pr1	Nor.	6.3.1	Pr3	E
	Pr2	Nor.	6.3.1	Pr1	E
	Pr3	Nor.	6.3.1	Pr2	E
5	Relation between the characteristics of the transmission system and safety procedures	Nor.	7.2.8		E
5.1	Functional integrity requirement (text up to P1)	Nor.	Not used		
	P1 to P5	Nor.	7.1	General	T
	P6	Nor.	7.2.5		E
5.2	Safety integrity requirements R1 to R6	Nor.	7.2	General requirements	T
6.1	General	Nor.	Not used		
6.2	Communication between safety related equipment	Nor.	7.1 and 7.2		T
6.3	Communication between safety related and non-safety related equipment	Nor.	7.2.2		E
			7.3.8.2.1		E
6.4	Communication between non-safety related equipment	Nor.	Not used		

(Sub)clause of IEC 62280-1:2002	Informative / Normative	(Sub)clause of IEC 62280	Unchanged / Modified
7.1 General requirements	Nor.	7.3.8.2.3	E
7.2 Safety target	Nor.	7.2.5	T
7.3 Length of safety code	Nor.	7.3.8.2.4	E
Annex A Length of safety code	Inf.	C.4 Length of safety code	U

Inf. Informative

Nor. Normative

U (unchanged) includes:
Changes of references and changes of terminology to achieve consistency of the whole standard.

E (editorial changes) includes:
No change of contents, only rearrangements and improvements.

T (technical changes) includes:
Contents either moved to other (sub)clauses or changed.

Table E.2 – Mapping from IEC 62280-2:2002 to IEC 62280

(Sub)clause of IEC 62280-2:2002	Informative / Normative	(Sub)clause of IEC 62280	Unchanged / Modified
Introduction	Inf.	Introduction	E
1 Scope	Nor.	1 Scope	E
2 Normative references	Nor.	2 Normative references	E
3 Definitions	Nor.	3 Terms, definitions and abbreviations	E
4 Reference architecture	Nor.	4 Reference architecture	T
5 Threats to the transmission system	Nor.	5 Threats to the transmission system	U
6.1 Introduction	Nor.	7.1 General	U
6.2 General requirements	Nor.	7.2 General requirements	T
6.3 Specific defences	Nor.	7.3 Specific defences	U
6.3.1 Sequence number	Nor.	7.3.2 Sequence number	U
6.3.2 Time stamp	Nor.	7.3.3 Time stamp	U
6.3.3 Time-out	Nor.	7.3.4 Time-out	U
6.3.4 Source and destination identifiers	Nor.	7.3.5 Source and destination identifiers	U
6.3.5 Feedback message	Nor.	7.3.6 Feedback message	U
6.3.6 Identification procedure	Nor.	7.3.7 Identification procedure	U
6.3.7 Safety code	Nor.	7.3.8 Safety code	T
6.3.8 Cryptographic techniques	Nor.	7.3.9 Cryptographic techniques	T
7.1 Introduction	Nor.	7.4.1 General	U
7.2 Threats/defences matrix	Nor.	7.4.2 Threats/defences matrix	U
7.3 Choice and use of safety code and cryptographic techniques	Nor.	7.4.3 Choice and use of safety code and cryptographic techniques	U
A.1 Applications of time stamps	Inf.	C.1 Applications of time stamps	U
A.2 Choice and use of safety codes and cryptographic techniques	Inf.	C.2 Choice and use of safety codes and cryptographic techniques	T
Bibliography	Inf.	Bibliography	T
C.1 Scope/purpose	Inf.	6.1 General	T

(Sub)clause of IEC 62280-2:2002	Informative / Normative	(Sub)clause of IEC 62280	Unchanged / Modified
C.2 Classification of transmission systems	Inf.	6.2 General aspects of classification	T
		Annex B Categories of transmission system	T
C.3 Procedure	Inf.	D.1 Procedure	U
C.4 Example	Inf.	D.2 Example	U
Annex D Threats on open transmission systems	Inf.	Annex A Threats on open transmission systems	E

Inf. Informative

Nor. Normative

U (unchanged) includes:
Changes of references and changes of terminology to achieve consistency of the whole standard.

E (editorial changes) includes:
No change of contents, only rearrangements and improvements.

T (technical changes) includes:
Contents either moved to other (sub)clauses or changed.

Bibliography

IEC 61025, *Fault Tree Analysis (FTA)*

ISO/IEC 9796-2:2010, *Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms*

ISO/IEC 9796-3:2006, *Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms*

ISO/IEC 9797-1:2011, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher*

ISO/IEC 9797-2:2011, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function*

ISO/IEC 10116:2006, *Information technology – Security techniques – Modes of operation for an n-bit block cipher*

ISO/IEC 10118-1:2000, *Information technology – Security techniques – Hash-functions – Part 1: General*

ISO/IEC 10118-2:2010, *Information technology – Security techniques – Hash-functions – Part 2: Hash-functions using an n-bit block cipher*

ISO/IEC 10118-3:2004, *Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions*

ISO/IEC 10118-4:1998, *Information technology – Security techniques – Hash-functions – Part 4: Hash-functions using modular arithmetic*

ISO/IEC 11770-1:2010, *Information technology – Security techniques – Key management – Part 1: Framework*

ISO/IEC 11770-2:2008, *Information technology – Security techniques – Key management – Part 2: Mechanisms using symmetric techniques*

ISO/IEC 11770-3:2008, *Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques*

UIC 738, *Processing and transmission of safety information*

UIC/ORE A155.1 Report RP 4, September 1984: *Survey of available measures for protection of safety information during transmission* (also available in German and French)

FIPS PUB 197, 26.11.2001: *Advanced Encryption Standard*

D.W. Davies and W.L. Price: *Security for Computer Networks,* 2nd edition, J. Wiley & Sons, Chichester

W.Wesley Peterson, *Error correction Codes*, M.I.T. Press, 1967

R. Rivest, *The MD4 Message-Digest Algorithm*, 4/92, published within Internet RFC 1320

Bruce Schneier, *Applied Cryptography*, J. Wiley & Sons, Inc, 2nd edition, 1995

A. Tanenbaum, *Distributed Systems*, Prentice Hall, 1995

Wolf, J. K., Michelson, A. M. und Levesque, A. H., *On the probability of undetected error for linear block codes,* IEEE Trans. Communication, vol.30, pp.317-325, 1982

IEEE COM-30, Dodunekova R., Dodunekov S. M., *Sufficient conditions for good and proper detecting codes,* IEEE Trans. Inform. Theory, vol. 43, pp. 2023-2026, 1997

IEEE Trans. Inform. Theory, vol. 43, pp. 2023-2026, Nov. 1997

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

APPLICATIONS FERROVIAIRES – SYSTÈMES DE SIGNALISATION, DE TÉLÉCOMMUNICATION ET DE TRAITEMENT – COMMUNICATION DE SÉCURITÉ DANS LES SYSTÈMES DE TRANSMISSION

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de la CEI. La CEI n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de brevet. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale CEI 62280 a été établie par le comité d'études 9 de la CEI: Matériels et systèmes électriques ferroviaires.

Cette norme est basée sur l'EN 50159.

La présente norme annule et remplace la CEI 62280-1 (2002) et la CEI 62280-2 (2002). Voir Annexe E.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
9/1866A/FDIS	9/1885/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de la CEI sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

INTRODUCTION

Si un système électronique relatif à la sécurité implique le transfert d'informations entre plusieurs emplacements, le système de transmission fait alors partie intégrante du système relatif à la sécurité. Il en découle que la communication de bout en bout est sécurisée, conformément à la CEI 62425.

Le système de transmission envisagé dans la présente norme qui sert au transfert d'informations entre différents emplacements n'a, de manière générale, aucune condition préalable particulière à remplir. Du point de vue de la sécurité, il est non approuvé ou non approuvé totalement.

La présente norme est consacrée aux exigences devant être prises en compte pour la communication d'informations relatives à la sécurité sur de tels systèmes de transmission.

Bien que cette norme ne traite pas de la mémoire RAM, il convient de garder à l'esprit qu'elle est un aspect essentiel de la sécurité globale.

Les exigences de sécurité dépendent des caractéristiques du système de transmission. Afin de réduire la complexité de l'approche visant à démontrer la sécurité du système, les systèmes de transmission ont été classifiés en trois catégories:

- La catégorie 1 regroupe les systèmes qui sont sous le contrôle du concepteur et réparés au cours de leur durée de vie.
- La catégorie 2 regroupe les systèmes qui sont partiellement inconnus ou non réparés, cependant l'accès non autorisé peut être exclu.
- La catégorie 3 regroupe les systèmes qui ne sont pas sous le contrôle du concepteur et pour lesquels l'accès non autorisé doit être envisagé.

La première catégorie était couverte par la CEI 62280-1:2002, les autres par la CEI 62280-2:2002.

Lorsque des systèmes de communication relatifs à la sécurité qui ont été approuvés conformément aux normes précédentes font l'objet de maintenance et/ou d'extensions, l'Annexe informative E peut être utilisée à des fins de traçabilité des articles ou paragraphes de la présente norme par rapport aux articles ou paragraphes de la série précédente.

APPLICATIONS FERROVIAIRES – SYSTÈMES DE SIGNALISATION, DE TÉLÉCOMMUNICATION ET DE TRAITEMENT – COMMUNICATION DE SÉCURITÉ DANS LES SYSTÈMES DE TRANSMISSION

1 Domaine d'application

La présente Norme internationale est applicable aux systèmes électroniques relatifs à la sécurité utilisant, à des fins de communication numérique, un système de transmission qui n'était pas nécessairement conçu pour des applications relatives à la sécurité et qui est:

- sous le contrôle du concepteur et réparé au cours de sa durée de vie, ou
- partiellement inconnu ou non réparé, mais pour lequel l'accès non autorisé peut être exclu, ou
- n'étant pas sous le contrôle du concepteur et pour lequel l'accès non autorisé doit être envisagé.

Des équipements relatifs à la sécurité et des équipements non relatifs à la sécurité peuvent être connectés au système de transmission.

La présente norme internationale donne les exigences de base nécessaires pour réaliser une communication relative à la sécurité entre des équipements relatifs à la sécurité connectés au système de transmission.

La présente norme internationale est applicable à la spécification des exigences de sécurité des équipements relatifs à la sécurité connectés au système de transmission, en vue d'obtenir les exigences d'intégrité de sécurité affectées.

Les exigences de sécurité sont généralement mises en œuvre dans les équipements relatifs à la sécurité conçus conformément à la CEI 62425. Dans certains cas, ces exigences peuvent être mises en œuvre dans d'autres équipements du système de transmission à conndition qu'il existe un contrôle par des mesures de sécurité pour satisfaire aux exigences d'intégrité de sécurité affectées.

La spécification des exigences de sécurité est une condition préalable du dossier de sécurité d'un système électronique relatif à la sécurité pour laquelle les preuves exigées sont définies dans la CEI 62425. Les preuves de la gestion de la sécurité et de la qualité doivent être issues de la CEI 62425. La présente norme concerne les exigences relatives à la communication pour les preuves de sécurité fonctionnelle et technique.

La présente norme internationale n'est pas applicable aux systèmes existants qui ont déjà été acceptés avant la publication de la présente norme.

La présente norme internationale ne spécifie pas:

- le système de transmission,
- les équipements connectés au système de transmission,
- les solutions (par exemple pour l'interopérabilité),
- les données qui sont relatives à la sécurité et celles qui ne le sont pas.

Un équipement relatif à la sécurité connecté via un système de transmission ouvert peut être soumis à de nombreuses menaces de sécurité informatique différentes contre lesquelles un programme global comprenant les aspects de gestion, techniques et opérationnels doit être défini.

Dans la présente norme internationale cependant, du point de vue de la sécurité informatique, seules les attaques intentionnelles par le biais de messages aux applications relatives à la sécurité sont envisagées.

La présente norme internationale ne couvre pas les problèmes généraux de sécurité informatique et ne couvre pas, en particulier, les problèmes de sécurité informatique relatifs à:

- la confidentialité des informations relatives à la sécurité,
- la surcharge du système de transmission.

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

CEI 62278-2 (toutes les parties), *Applications ferroviaires – Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS)*

CEI 62425:2007, *Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Systèmes électroniques de sécurité pour la signalisation*

3 Termes, définitions et abréviations

3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

3.1.1
date absolue
date référencée par rapport à un temps global, commun à un groupe d'entités utilisant un réseau de transmission

3.1.2
protection d'accès
processus conçus pour empêcher un accès non autorisé de lire ou de modifier de l'information, soit dans les systèmes de sécurité, soit dans le système de transmission

3.1.3
données additionnelles
données inutiles pour les processus utilisateur finals, mais utilisées à des fins de contrôle, de disponibilité et de sécurité

3.1.4
message authentique
message dont l'information est reconnue provenir de la source indiquée

3.1.5
authenticité
état dans lequel une information est valide et réputée avoir été générée par la source déclarée

3.1.6
système de transmission fermé
nombre fixe ou nombre maximal fixe d'éléments reliés par un système de transmission dont les propriétés sont connues et fixées et où le risque d'accès non autorisé est considéré comme négligeable

3.1.7
communication
transfert d'informations entre des applications

3.1.8
confidentialité
propriété de non-mise à disposition de l'information à des entités non autorisées

3.1.9
corruption de message
type d'erreur de message dans lequel se produit une altération des données

3.1.10
techniques cryptographiques
les données de sortie sont calculées au moyen d'un algorithme utilisant les données d'entrée et une clé comme paramètre

Note 1 à l'article: Connaissant les données de sortie, il est impossible de calculer les données d'entrée dans un délai raisonnable sans connaître la clé. Il est également impossible de déduire la clé des données de sorties dans un délai raisonnable, même si les données d'entrée sont connues.

3.1.11
contrôle de redondance cyclique
code cyclique utilisé pour protéger les messages de l'influence de la corruption des données

3.1.12
données
partie d'un message qui représente de l'information

Note 1 à l'article: Voir aussi les définitions 3.1.64: données utilisateur, 3.1.3 données additionnelles et 3.1.42: données redondantes.

3.1.13
corruption de données
altération de données

3.1.14
défense
mesure introduite dans la conception du système de communications de sécurité pour contrer des menaces particulières

3.1.15
retard de message
type d'erreur de message dans lequel un message est reçu plus tard que prévu

3.1.16
suppression de message
type d'erreur de message dans lequel un message est retiré d'un flux de messages

3.1.17
date double
cas où deux entités échangent et comparent leurs dates. Dans ce cas, les dates des entités sont indépendantes entre elles

3.1.18
erreur
écart par rapport à la conception prévue pouvant conduire à une défaillance ou à un comportement inattendu du système

3.1.19
défaillance
écart par rapport aux performances spécifiées d'un système

Note 1 à l'article: Une défaillance est la conséquence d'un défaut ou d'une erreur dans un système.

3.1.20
défaut
état anormal pouvant conduire à une erreur ou à une défaillance dans un système

Note 1 à l'article: Un défaut peut être aléatoire ou systématique.

3.1.21
message en retour
réponse d'un récepteur à l'émetteur, via un canal de transmission en retour

3.1.22
hacker
personne essayant de shunter délibérément une protection d'accès

3.1.23
danger
condition qui peut conduire à un accident

3.1.24
analyse des dangers
processus d'identification des situations dangereuses et d'analyse de leurs causes, ainsi que les écarts par rapport aux exigences pour limiter la probabilité d'occurrence et les conséquences des situations dangereuses à un niveau acceptable

3.1.25
données implicites
données additionnelles qui ne sont pas transmises, mais sont connues de l'émetteur et du récepteur

3.1.26
information
représentation de l'état ou des événements d'un processus, dans une forme compréhensible par le processus

3.1.27
insertion de message
type d'erreur de message dans lequel un message est ajouté dans le flux de messages

3.1.28
intégrité
état dans lequel une information est complète et non altérée

3.1.29
code de détection de manipulation
fonction de tout le message sans clé secrète

Note 1 à l'article: Par opposition au MAC, aucune clé secrète n'est impliquée. Par tout le message, on comprend également toute donnée implicite du message qui n'est pas envoyé au système de transmission. Le MDC est souvent basé sur une fonction de brouillage.

3.1.30
mascarade de message
insertion d'un message non authentique, déguisé pour passer pour authentique

3.1.31
message
information qui est transmise par un émetteur (source de données) à un ou plusieurs récepteurs (collecteur de données)

3.1.32
code d'authentification de message
fonction cryptographique de tout le message et d'une clé secrète ou publique

Note 1 à l'article: Par tout le message, on comprend également toute donnée implicite du message qui n'est pas envoyé au système de transmission.

3.1.33
cryptage de message
transformation de bits en appliquant une technique de cryptage à un message, suivant un algorithme piloté par clés, afin de rendre plus difficile une lecture fortuite des données. Ne protège pas contre la corruption des données

3.1.34
erreurs de message
ensemble de tous les modes de défaillance de message possibles, ce qui peut conduire à des situations potentiellement dangereuses ou à une réduction de la disponibilité du système. Plusieurs causes peuvent être associées à un type d'erreur donné

3.1.35
intégrité du message
message dans lequel l'information est complète et non altérée

3.1.36
flux de messages
suite ordonnée de messages

3.1.37
code de sécurité non cryptographique
données redondantes, basées sur des fonctions non cryptographiques, incluses dans un message de sécurité, afin de rendre possible la détection de la corruption des données, par la fonction de transmission de sécurité

3.1.38
système de transmission ouvert
système de transmission à nombre d'utilisateurs inconnu, ayant des propriétés non connues, variables et dans lesquelles on ne peut avoir confiance, utilisé pour des services de télécommunication inconnus et pour lequel il existe un risque d'accès non autorisé

3.1.39
réseau public
réseau ayant des utilisateurs inconnus, en particulier non soumis au contrôle ferroviaire

3.1.40
défaillance aléatoire
une défaillance qui se produit aléatoirement dans le temps

3.1.41
contrôle de redondance
type de contrôle de l'existence d'une relation prédéfinie entre la redondance et les données utilisateur au sein d'un message, pour prouver l'intégrité du message

3.1.42
données redondantes
données additionnelles dérivées des données utilisateur, par un processus de transmission de sécurité

3.1.43
date relative
date référencée par rapport à l'horloge locale d'une entité. En général, il n'y a pas de relation avec les horloges des autres entités

3.1.44
répétition de message
type d'erreur de message dans lequel un message unique est reçu plus d'une fois

3.1.45
reséquencement de messages
type d'erreur de message dans lequel l'ordre des messages est modifié dans le flux de messages

3.1.46
état de secours sûr
état sûr d'un équipement ou d'un système relatif à la sécurité comme déviation par rapport à un état normal et comme résultat d'une réaction de protection conduisant à une fonctionnalité réduite des fonctions relatives à la sécurité, voire également des fonctions non relatives à la sécurité

3.1.47
sécurité
absence de risque inacceptable

3.1.48
dossier de sécurité
document dans lequel est consigné l'ensemble des démonstrations prouvant que le produit (par exemple système/sous-système/équipement) satisfait aux exigences de sécurité spécifiées

3.1.49
code de sécurité
données redondantes incluses dans un message de sécurité afin de détecter la corruption des données par la fonction de transmission de sécurité

3.1.50
niveau d'intégrité de la sécurité
nombre qui indique le degré de confiance exigé pour qu'un système satisfasse à ses fonctions de sécurité spécifiées eu égard à ses défaillances systématiques

3.1.51
réaction de protection
action prise par le processus de sécurité en réponse à un événement (comme une défaillance du système de communication) qui peut conduire à un état de secours sûr de l'équipement

3.1.52
relatif à la sécurité
qui est responsable de la sécurité

3.1.53
fonction de transmission relative à la sécurité
fonction intégrée à l'équipement relatif à la sécurité qui garantit l'authenticité, l'intégrité, la ponctualité et l'ordre des données

3.1.54
numéro de séquence
un champ de donnée additionnel contenant un nombre qui varie d'une manière prédéfinie de message à message

3.1.55
identificateur de source et de destination
un identificateur est assigné à chaque entité. L'identificateur peut être un nom, un nombre ou un motif de bits arbitraire. L'identificateur sera utilisé pour une transmission de sécurité. L'identificateur est rajouté d'habitude aux données utilisateur

3.1.56
défaillance systématique
une défaillance d'occurrence répétitive moyennant des combinaisons particulières d'entrée ou des conditions particulières d'environnement

3.1.57
menace
violation potentielle de la sécurité

3.1.58
datation
information relative au temps de la transmission attachée au message par l'émetteur

3.1.59
ponctualité
état correspondant à une mise à disposition de l'information au bon moment conformément aux exigences

3.1.60
code de transmission
information redondante, ajoutée au message de sécurité ou d'une autre nature du système de transmission non sécurisé pour assurer l'intégrité du message pendant la transmission

3.1.61
système de transmission
service faisant appel à la communication de blocs de message entre un nombre de participants, qui peuvent être des sources ou des collecteurs d'information

3.1.62
fiable
qui a des propriétés utilisées comme preuve pour étayer la démonstration de sécurité

3.1.63
accès non autorisé
situation dans laquelle des personnes non autorisées ou des hackers ont accès à et/ou modifient de l'information utilisateur ou de l'information dans le système de transmission

3.1.64
données utilisateur
données représentant les états ou événements d'un processus utilisateur, sans données additionnelles. Dans le cas d'une communication entre des équipements de sécurité, les données utilisateur contiennent des données de sécurité

3.1.65
message valide
message qui satisfait dans sa forme à toutes les exigences spécifiées par l'utilisateur

3.1.66
validité
état de satisfaction aux exigences spécifiées par l'utilisateur

3.2 Abréviations

BCH	Code Bose, Ray-Chaudhuri, Hocquenghem
BME	Basic Message Errors (erreurs de message basiques)
BSC	Binary Symmetric Channel (canal binaire symétrique)
CAN	Controller Area Network (réseau CAN)
CRC	Contrôle de redondance cyclique
EC	Communauté européenne
ECB	Electronic CodeBook mode (mode dictionnaire de codes)
EMI	Electromagnetic Interference (perturbation électromagnétique)
FTA	Fault Tree Analysis (analyse par arbre des causes)
GPRS	General Packet Radio Service (service de paquet radio général)
GSM-R	Global System for Mobile communication - Railways (système global de communication mobile - chemins de fer)
ED	Evénements dangereux
HW	Hardware (matériel)
IT	Information Technology (informatique)
LAN	Local Area Network (réseau local)
MAC	Message Authentification Code (code d'authentification de message)
MDC	Manipulation Detection code (code de détection de manipulation)
MD4, MD5	Message Digest algorithms (algorithmes de traitement de message)
DP	Danger Principal
MTBF	Mean Time Between Failures (temps moyen entre défaillances)
MVB	Multi-purpose Vehicle Bus (bus de véhicule multifonctions)

PROFIBUS	Process Field Bus (bus de champ de traitement)
QSC	q-nary symmetric channel (canal q-aire symétrique)
RAMS	Fiabilité, disponibilité, maintenabilité et sécurité
SIL	Safety Integrity Level (niveau d'intégrité de la sécurité)
SR	Safety Related (relatif à la sécurité)
SRS	Safety Requirements Specifications (spécification des exigences de sécurité)
SW	Software (logiciel)
TX	Transmission
UTC	Universal Coordinated Time (temps universel coordonné)
WAN	Wide Area Network (réseau global)
Wi-Fi	Wireless Fidelity (réseau sans fil)

4 Architecture de référence

La présente norme internationale définit les exigences de sécurité pour la sécurité des communications entre des équipements relatifs à la sécurité via un système de transmission qui peut être fermé ou ouvert. Des équipements relatifs à la sécurité et des équipements non relatifs à la sécurité peuvent être connectés au système de transmission. Le présent article décrit les configurations possibles des communications relatives à la sécurité dans les systèmes de transmission et comprend la définition des blocs fonctionnels impliqués. Les exigences particulières qui doivent être satisfaites par ces blocs sont indiquées dans les articles suivants.

Une vue combinée de l'architecture principale pour les systèmes de transmission ouverts et fermés est présentée à la Figure 1 dans laquelle tous les éléments sont reliés conformément au flux d'information pour l'échange d'informations relatives à la sécurité entre des équipements relatifs à la sécurité. L'architecture de référence présente également une interface non relative à la sécurité qui n'est pas toujours présente. Une utilisation classique pourrait être pour l'acheminement des messages de diagnostic vers un centre de maintenance.

Outre la source et la destination des communications relatives à la sécurité, l'architecture de référence traite d'un système de communication relatif à la sécurité qui peut être divisé en:

- fonctions de transmissions relatives à la sécurité incorporées aux équipements relatifs à la sécurité. Ces fonctions garantissent l'authenticité, l'intégrité, la ponctualité et l'ordre des données,
- techniques cryptographiques relatives à la sécurité qui protègent le message relatif à la sécurité. Celles-ci peuvent être mises en œuvre en les incorporant aux équipements relatifs à la sécurité ou en les situant à l'extérieur des équipements relatifs à la sécurité tout en les contrôlant par des techniques de sécurité. Ces techniques protègent le message relatif à la sécurité dans un système de transmission de catégorie 3 et ne sont pas nécessaires dans un système de transmission de catégorie 1 ou 2,
- un système de transmission ouvert ou fermé non relatif à la sécurité qui peut lui-même inclure des fonctions de protection des transmissions et/ou accéder à des fonctions de protection.

Les caractéristiques des systèmes de transmission fermés (catégorie 1) sont les suivantes:

- le nombre de pièces d'équipement connectables, qu'elles soient relatives à la sécurité ou non, au système de transmission est connu et fixé;
- le risque d'accès non autorisé est considéré négligeable;
- les caractéristiques physiques du système de transmission (par exemple les supports de transmission, l'environnement par rapport aux hypothèses de conception, etc.) sont fixées et ne varient pas au cours du cycle de vie du système.

Le système de transmission ouvert (catégorie 2 et/ou 3) peut contenir tout ou partie des éléments suivants:

- éléments qui lisent, stockent, traitent ou retransmettent les données produites et présentées par les utilisateurs du système de transmission, conformément à un programme inconnu de l'utilisateur. Le nombre d'utilisateurs est généralement inconnu et les équipements relatifs à la sécurité ou non, ainsi que les équipements qui ne sont pas relatifs aux applications ferroviaires, peuvent être connectés au système de transmission ouvert;
- supports de transmission de tout type avec des caractéristiques de transmission et une sensibilité aux influences externes qui sont inconnues de l'utilisateur;
- systèmes de contrôle et de gestion du réseau capables d'acheminer (et de réacheminer dynamiquement) des messages via n'importe quel itinéraire constitué d'un ou plusieurs types de supports de transmission entre les extrémités du système de transmission ouvert, conformément à un programme inconnu de l'utilisateur;
- autres utilisateurs du système de transmission, inconnus du concepteur de l'application relative à la sécurité, envoyant des quantités inconnues de données dans des formats inconnus.

Le système de transmission ouvert de catégorie 3 peut être sujet à des accès non autorisés à des fins malveillantes.

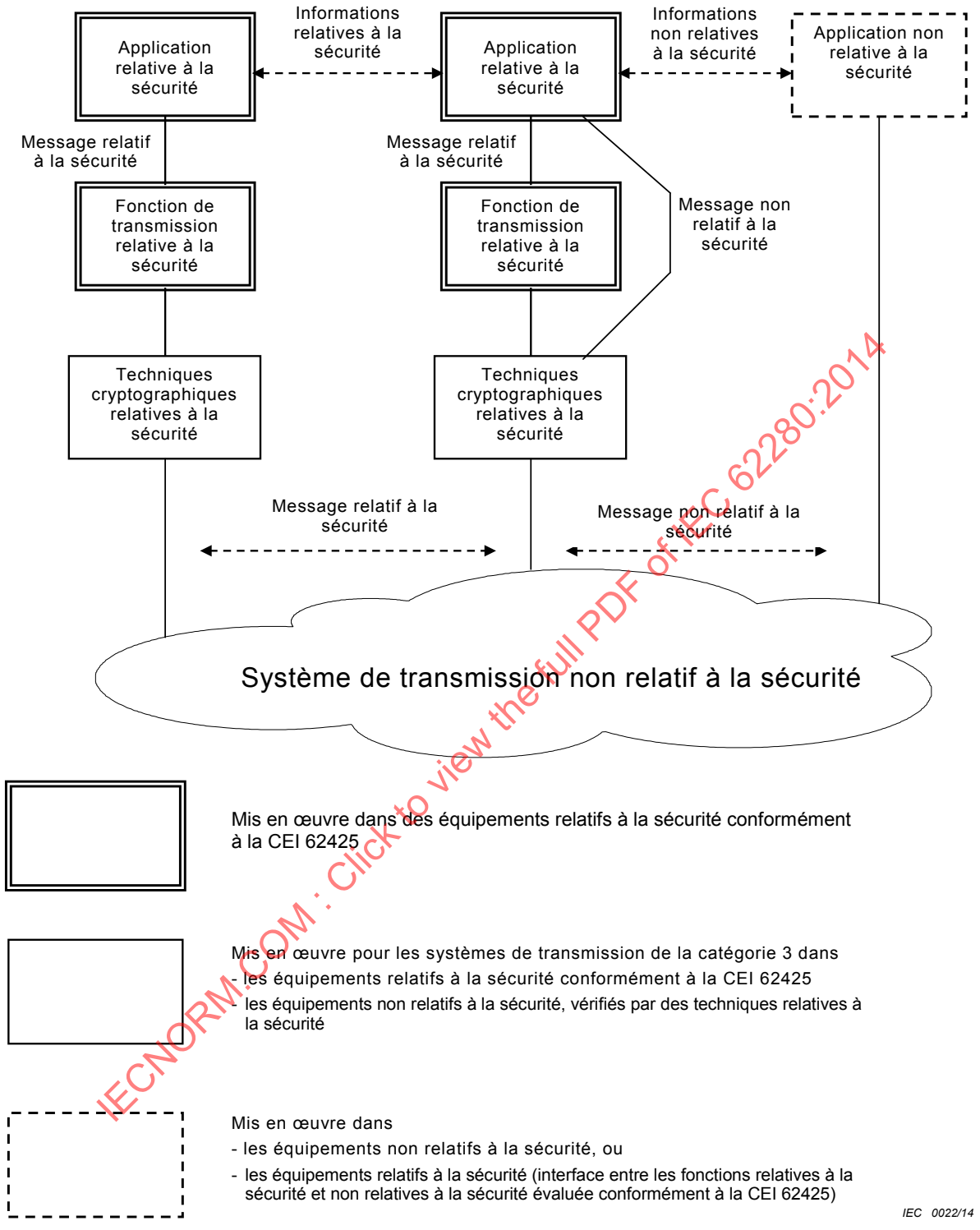


Figure 1 – Architecture de référence pour les communications relatives à la sécurité

L'architecture de référence ne vise pas à restreindre les possibilités de mise en œuvre; différentes structures sont possibles, voir les exemples dans l'Annexe informative C et en particulier à l'Article C.5 pour les messages non relatifs à la sécurité.

5 Menaces pour le système de transmission

Le danger principal des communications relatives à la sécurité est l'échec à obtenir un message valide en termes d'authenticité, d'intégrité, d'ordre et de ponctualité à l'extrémité réceptrice. Cette norme considère les menaces sur ces propriétés de message qui émanent du système de transmission. Les menaces sur les équipements relatifs à la sécurité doivent être envisagées conformément à la CEI 62425.

Cependant, la satisfaction aux exigences de la présente norme ne fournit pas de protection contre la mauvaise utilisation, intentionnelle ou non intentionnelle, par des sources autorisées. Il est nécessaire d'aborder ces aspects dans le dossier de sécurité.

Des informations supplémentaires, ainsi que des lignes directrices sur l'analyse des menaces et le dossier de sécurité, sont fournies dans l'Annexe informative A. On doit insister sur le fait que l'analyse doit être réalisée pour chaque projet. La méthodologie pour les erreurs de message de l'Annexe A peut donc être incluse, mais elle ne sera pas nécessairement exhaustive en elle-même.

Les événements dangereux identifiés peuvent être les suivants:

- défaillance systématique;
- rupture de câbles;
- erreurs de câblage;
- désalignement d'antenne;
- perte de performance;
- défaillance aléatoire et vieillissement du HW (matériel);
- erreur humaine;
- erreur de maintenance;
- EMI (perturbation électromagnétique);
- paradiaphonie;
- bruit thermique;
- effets d'évanouissement;
- surcharge du système de transmission;
- orage magnétique;
- incendie;
- séisme;
- foudre

ainsi que des événements causés délibérément tels que:

- branchements clandestins,
- HW endommagé ou modifié sans autorisation,
- SW modifié sans autorisation,
- contrôle des canaux,
- transmission de messages non autorisés.

Cependant, si de nombreux événements dangereux différents peuvent survenir, les erreurs de message basiques qui constituent les menaces pesant sur le système de transmission sont les suivantes:

- répétition;

- suppression;
- insertion;
- reséquencement;
- corruption;
- retard;
- mascarade.

Le Tableau A.1 suggère quelles menaces pour le système de transmission peuvent être causées par chaque type d'événement dangereux. Une fois que les événements dangereux pour lesquels aucun moyen de protection n'est prévu et qui peuvent survenir pour un système particulier sont identifiés, le tableau peut servir de guide pour identifier les menaces à envisager pour ce système.

Le Tableau A.1 ne contient pas la probabilité d'occurrence; cet aspect doit faire partie de l'analyse des menaces.

6 Classification des systèmes de transmission

6.1 Généralités

Le présent article définit le processus devant être utilisé pour classifier tous les systèmes de transmission et identifie les menaces pertinentes pour de tels systèmes qui affectent le choix des défenses à inclure dans l'application de sécurité.

6.2 Aspects généraux de la classification

Il existe de nombreux facteurs qui peuvent influencer les menaces pesant sur un système de communication relatif à la sécurité.

Il est par exemple possible que les services de transmission puissent être obtenus par l'utilisateur du système de signalisation de la part des fournisseurs de services de télécommunication privés ou publics. Avec de tels contrats de mise à disposition de service, la responsabilité du fournisseur de service dans la garantie des performances du système de transmission peut être limitée.

La signification des menaces (et donc les exigences en matière de défenses) dépend donc de l'étendue du contrôle exercé par l'utilisateur sur le système de transmission, en tenant compte des problèmes suivants:

- les propriétés techniques du système, y compris les garanties de fiabilité ou de disponibilité du système, l'étendue du stockage des données inhérent au système (qui peut affecter le retard ou le reséquencement des messages);
- la cohérence des performances du système au cours de sa vie (par exemple lorsque des modifications sont apportées au système et à la base utilisateur), et les effets causés par la charge de trafic issue d'autres utilisateurs;
- l'accès au système, selon le caractère privé ou public du réseau, le degré de contrôle d'accès exercé par l'opérateur sur les autres utilisateurs, les opportunités de mauvaise utilisation du système par d'autres utilisateurs et la disponibilité de l'accès pour les personnes de la maintenance chargées de reconfigurer le système ou d'obtenir l'accès au support de transmission lui-même.

En fonction de ces problèmes, trois catégories de systèmes de transmission peuvent être définies.

6.3 Critères de classification des systèmes de transmission

6.3.1 Critères pour les systèmes de transmission de catégorie 1

Un système de transmission peut être considéré comme appartenant à la catégorie 1 si les conditions préalables suivantes sont remplies.

Pr1 Le nombre de pièces d'équipement, qu'elles soient relatives à la sécurité ou non, connectables au système de transmission est connu et fixé. Etant donné que les communications relatives à la sécurité dépendent de ce paramètre, le nombre maximal de participants autorisés à communiquer ensemble doit être indiqué dans la spécification des exigences de sécurité comme condition préalable. La configuration du système doit être définie/intégrée dans le dossier de sécurité. Tout changement ultérieur de cette configuration doit être précédé d'une vérification de ses effets dans le dossier de sécurité.

Pr2 Les caractéristiques du système de transmission (par exemple les supports de transmission, l'environnement dans les conditions les plus pénalisantes, etc.) sont connues et fixées. Elles doivent être maintenues tout au long du cycle de vie du système. Si des paramètres majeurs qui étaient utilisés dans le dossier de sécurité doivent être modifiés, tous les aspects relatifs à la sécurité doivent être vérifiés.

Pr3 Le risque d'accès non autorisé au système de transmission doit être négligeable.

Si un système de transmission remplit les conditions préalables ci-dessus, il peut être considéré comme appartenant à la catégorie 1 et comme étant un système fermé. Le cas échéant, il doit se conformer à un ensemble généralement restreint de processus et d'exigences fournis dans l'Article 7.

6.3.2 Critères pour les systèmes de transmission de catégorie 2

Si un système de transmission ne remplit pas les conditions préalables 1 ou 2 (Pr1 ou Pr2) de 6.3.1, mais remplit la condition préalable 3 (Pr3), il doit être considéré comme appartenant à la catégorie 2 et étant un système ouvert, et doit donc être évalué avec un ensemble plus large de processus et d'exigences fourni à l'Article 7.

6.3.3 Critères pour les systèmes de transmission de catégorie 3

Si un système de transmission ne remplit pas la condition préalable 3 (Pr3) de 6.3.1, il doit être considéré comme appartenant à la catégorie 3 et étant un système ouvert, et doit donc être évalué avec l'ensemble complet des processus et exigences fourni à l'Article 7.

6.4 Relation entre les systèmes de transmission et les menaces

La signification des menaces pour le système de communication relatif à la sécurité doit être évaluée en fonction de l'étendue du contrôle exercé par l'utilisateur sur le système de transmission.

Les menaces identifiées dans l'Article 5 sont applicables à toutes les catégories de systèmes de transmission à l'exception de la mascarade qui n'est applicable qu'aux systèmes de transmission ouverts.

Dans l'Annexe B, un exemple de classification des systèmes de transmission est donné au Tableau B.1 et un exemple de relation menace/catégorie est donné au Tableau B.2.

L'applicabilité de l'Article 7 dépend de la catégorie du système de transmission.

7 Exigences relatives aux défenses

7.1 Généralités

Par le passé, certaines techniques ont été adoptées dans les systèmes de transmission de données (relatifs à la sécurité ou non). Ces techniques constituent une "bibliothèque" des méthodes possibles qui est accessible au concepteur du système de contrôle et de protection pour pouvoir fournir une protection contre toutes les menaces identifiées plus haut.

Afin de réduire tout risque associé aux menaces identifiées dans l'article précédent, les services de sécurité fondamentaux suivants doivent être envisagés et fournis au niveau requis pour l'application, à la fois pour les systèmes de transmission ouverts et fermés:

- authenticité du message;
- intégrité du message;
- ponctualité du message;
- ordre du message.

L'ensemble suivant de défenses connues a été indiqué:

a) numéro de séquence;
b) datation;
c) temporisation;
d) identificateurs de source et de destination;
e) message en retour;
f) procédure d'identification;
g) code de sécurité;
h) techniques cryptographiques.

Un certain nombre de problèmes architecturaux doit être envisagé en fonction de l'application particulière et justifié dans le dossier de sécurité, par exemple

- les conditions de réclamations et de maintenance relatives à la conformité aux conditions préalables des catégories 1 ou 2 des systèmes de transmission,
- les critères pour la séparation entre systèmes de transmission de différentes catégories,
- la résistance des systèmes de transmission au déni de service consécutif aux attaques par "flooding", par exemple le besoin de pare-feu.

Concernant h), le domaine d'application de la présente norme exclut les problèmes généraux de sécurité informatique:

- seules les attaques survenant au cours de la phase opérationnelle sont prises en compte;
- seules les attaques exécutées au moyen de messages vers les applications relatives à la sécurité sont traitées ici.

Cependant, il convient qu'une politique de protection complète de l'accès envisage:

- les aspects procéduraux et de maintenance de la protection d'accès,
- la vulnérabilité des logiciels qui ne font pas partie de l'application relative à la sécurité,
- la confidentialité des informations.

7.2 Exigences générales

7.2.1 Des défenses adéquates doivent être fournies contre toutes les menaces identifiées pesant sur la sécurité des systèmes utilisant un système de transmission ouvert ou fermé.

Toute suspicion de menace devant être ignorée doit être justifiée et enregistrée dans le dossier de sécurité. L'Annexe A propose une liste possible des menaces qui doit être utilisée comme guide.

7.2.2 En cas de communication entre applications relatives à la sécurité et applications non relatives à la sécurité via le même système de transmission, les exigences suivantes s'appliquent:

- les défenses de sécurité mises en œuvre dans les fonctions de transmission relatives à la sécurité doivent être indépendantes fonctionnellement des défenses utilisées par les fonctions non relatives à la sécurité;
- les messages relatifs à la sécurité et les messages non relatifs à la sécurité doivent avoir des structures différentes obtenues par l'application d'un code de sécurité aux messages relatifs à la sécurité. Ce code de sécurité doit être en mesure de protéger le système au niveau d'intégrité de la sécurité exigé (voir 7.3.8) de sorte qu'un message non relatif à la sécurité ne peut pas être corrompu en message relatif à la sécurité.

7.2.3 Les exigences détaillées des défenses nécessaires pour l'application doivent prendre en compte:

- le niveau de risque (fréquence/conséquence) identifié pour chaque menace particulière, et
- le niveau d'intégrité de la sécurité des données et processus concernés.

L'Annexe C fournit des lignes directrices pour la sélection des techniques connues à l'heure actuelle pour assurer la défense contre les menaces. Il convient d'envisager avec attention les problèmes d'efficacité traités dans cette annexe lors du choix de la défense.

7.2.4 Les exigences pour les défenses nécessaires doivent être incluses dans la spécification des exigences du système et dans la spécification des exigences de sécurité du système pour l'application. Elles doivent constituer l'entrée de la portion "garantie de fonctionnement correct" du dossier de sécurité de l'application.

7.2.5 Toutes les défenses doivent être mises en œuvre conformément aux exigences définies dans la CEI 62425. Cela implique que les défenses:

- doivent être mises en œuvre entièrement dans l'équipement de transmission relatif à la sécurité (à l'exception possible de certaines architectures cryptographiques, voir 7.3.9 et l'Article C.2),
- doivent être indépendantes fonctionnellement des couches utilisées dans les systèmes de transmission non fiables.

7.2.6 Les exigences obligatoires pour les défenses particulières sont fournies dans les paragraphes suivants. Elles s'appliquent lorsque la défense particulière est utilisée.

7.2.7 D'autres défenses que celles décrites dans la présente norme peuvent être utilisées à condition que l'analyse de leur efficacité contre les menaces soit incluse dans le dossier de sécurité.

7.2.8 La preuve de la sécurité fonctionnelle et technique doit suivre le processus indiqué dans la CEI 62425, y compris:

- un modèle d'erreur global,
- une spécification fonctionnelle basée sur l'analyse du modèle d'erreur global,
- l'analyse de chaque défense utilisée dans la communication relative à la sécurité,
- la réaction de protection en cas de détection d'une erreur de transmission,
- une spécification des exigences d'intégrité de la sécurité et une affectation de SIL.

7.2.9 Le paragraphe 7.3 définit un ensemble exhaustif de défenses. Cependant, pour les systèmes de transmission de catégorie 1, l'ensemble restreint suivant est suffisant et maintient les services de sécurité fondamentaux:

- identifiants de source et/ou de destination (s'il y a plus d'un émetteur et/ou plus d'un récepteur);
- numéro de séquence et/ou datation au niveau requis par l'application; et
- code de sécurité.

7.3 Défenses spécifiques

7.3.1 Généralités

Les paragraphes suivants présentent de brèves introductions et les exigences propres à certaines défenses spécifiques qui sont efficaces individuellement ou en combinaison contre des menaces seules ou combinées. Toutes les exigences générales énumérées plus haut doivent être appliquées.

Des descriptions plus détaillées des défenses et de leur relation avec toutes les menaces possibles sont fournies dans l'Annexe informative C.

7.3.2 Numéro de séquence

7.3.2.1 Généralités

La numérotation de séquence consiste à ajouter un nombre courant (appelé numéro de séquence) à tous les messages échangés entre un transmetteur et un récepteur. Cela permet au récepteur de vérifier la séquence de messages fournis par le transmetteur.

7.3.2.2 Exigences

Le dossier de sécurité doit démontrer le caractère approprié des éléments suivants par rapport au niveau d'intégrité de la sécurité du processus et la nature du processus relatif à la sécurité:

- la longueur du numéro de séquence;
- la disposition relative à l'initialisation et au roulement du numéro de séquence;
- la disposition relative à la récupération à la suite d'une interruption de la séquence de messages.

7.3.3 Datation

7.3.3.1 Généralités

Lorsqu'une entité reçoit des informations, la signification des informations est souvent liée au temps. Le degré de dépendance entre informations et temps peut différer entre les applications. Dans certains cas, les informations anciennes peuvent être inutiles et inoffensives, mais dans d'autres cas, les informations sont susceptibles de représenter un danger potentiel pour l'utilisateur. En fonction du comportement temporel des processus qui échangent des informations (cyclique, contrôlé par les événements, etc.) la solution peut varier.

Une solution couvrant les relations temps-informations consiste à ajouter des datations aux informations. Ce type d'information peut être utilisé à la place de ou en combinaison avec les numéros de séquence, en fonction des exigences de l'application. Différentes utilisations de la datation et ses propriétés sont présentées à l'Article C.1.

7.3.3.2 Exigences

Le dossier de sécurité doit démontrer le caractère approprié des éléments suivants par rapport au niveau d'intégrité de la sécurité du processus et la nature du processus relatif à la sécurité:

- la valeur de l'incrément de temps;
- la précision de l'incrément de temps;
- la taille du temporisateur;
- la valeur absolue du temporisateur (par exemple UTC (temps universel coordonné) ou toute autre horloge mondiale);
- le synchronisme des temporisateurs dans les différentes entités;
- le temps écoulé entre l'émission de l'information et l'ajout d'une datation;
- le temps écoulé entre la vérification de la datation et l'utilisation de l'information.

7.3.4 Temporisation

7.3.4.1 Généralités

Dans les transmissions (généralement cycliques), le récepteur peut vérifier si le temps écoulé entre deux messages dépasse un temps maximal permis défini à l'avance. Si cela est le cas, une erreur doit être présumée (voir Figure 2).

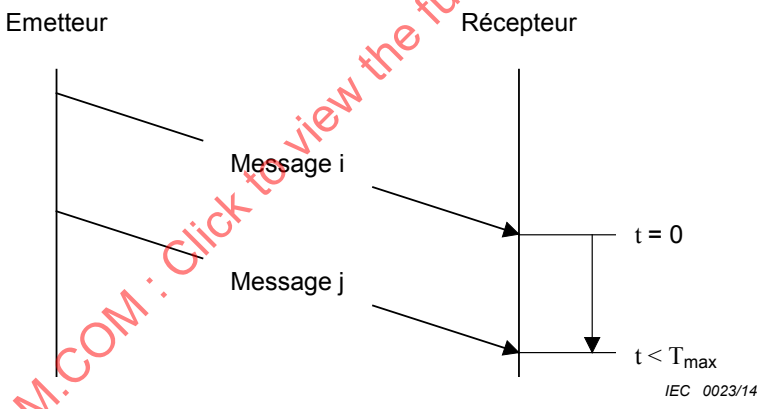


Figure 2 – Transmission cyclique des messages

Si un canal de retour est disponible, la supervision peut être effectuée par l'émetteur. L'émetteur démarre un temporisateur au moment d'envoyer un message i. Le récepteur du message i répond par un message reconnu j relatif au message reçu i. Si l'émetteur ne reçoit pas le message reconnu correspondant j en un laps de temps prédéfini, une erreur doit être présumée (voir Figure 3).

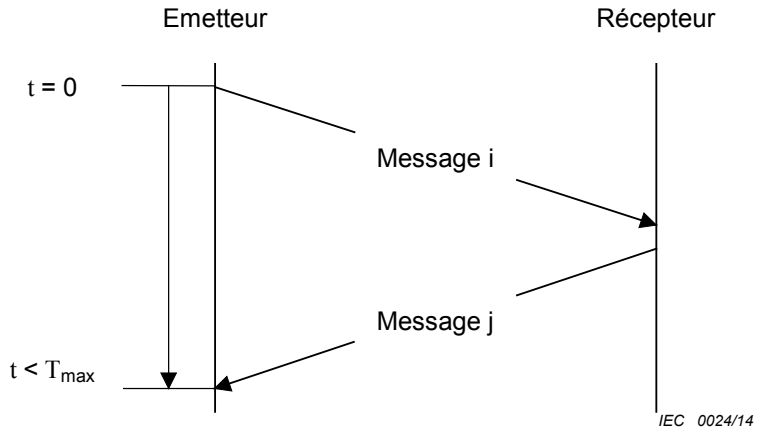


Figure 3 – Transmission bidirectionnelle des messages

7.3.4.2 Exigences

Le dossier de sécurité doit démontrer le caractère approprié des éléments suivants par rapport au niveau d'intégrité de la sécurité du processus et la nature du processus relatif à la sécurité:

- le retard acceptable;
- la précision de la temporisation.

7.3.5 Identificateurs de source et de destination

7.3.5.1 Généralités

Les processus de communication entre plusieurs parties nécessitent des moyens pour vérifier la source de toutes les informations reçues avant qu'elles soient utilisées. Pour ce faire, les messages doivent inclure des données additionnelles.

Les messages peuvent contenir un identifiant unique de la source ou un identifiant unique de la destination ou les deux. Le choix est fait en fonction de l'application relative à la sécurité. Ces identifiants sont ajoutés aux fonctions de transmission relatives à la sécurité de l'application.

- L'inclusion d'un identifiant de la source dans les messages peut permettre aux utilisateurs des messages de vérifier que les messages proviennent bien de la source voulue, sans nécessiter pour autant de dialogue entre l'émetteur et le récepteur. Cela peut être utile, par exemple dans les communications unidirectionnelles ou les diffusions.
- L'inclusion d'un identifiant de la destination dans les messages peut permettre aux utilisateurs des messages de vérifier que les messages leur sont bien destinés, sans nécessiter pour autant de dialogue entre l'émetteur et le récepteur. Cela peut être utile, par exemple dans les communications unidirectionnelles ou les diffusions. Les identifiants de destination peuvent être choisis pour identifier des destinations individuelles ou des groupes d'utilisateurs.

7.3.5.2 Exigences

Le dossier de sécurité doit démontrer le caractère approprié des éléments suivants par rapport au niveau d'intégrité de la sécurité du processus et la nature du processus relatif à la sécurité:

- l'unicité des identifiants des entités dans l'ensemble du système de transmission;
- la taille du champ de données de l'identifiant.

7.3.6 Message en retour

7.3.6.1 Généralités

Lorsqu'un canal de transmission en retour approprié est disponible, un message en retour peut être envoyé de la part du récepteur des informations critiques du point de vue de la sécurité à l'émetteur. Le contenu de ce message en retour peut inclure:

- des données dérivées du contenu du message original, dans une forme identique ou altérée,
- des données ajoutées par le récepteur, dérivées de ses propres informations locales,
- des données additionnelles à des fins de sécurité et de sûreté.

L'utilisation d'un tel message en retour peut contribuer à la sécurité du processus de multiples façons:

- en fournissant la confirmation concrète de la réception de messages valides et ponctuels;
- en fournissant la confirmation concrète de la réception de messages corrompus afin de permettre la prise de mesures appropriées;
- en confirmant l'identité de l'équipement récepteur;
- en facilitant la synchronisation des horloges entre les équipements émetteur et récepteur;
- en facilitant les procédures de vérification dynamique entre les parties.

7.3.6.2 Exigences

L'existence d'un canal de retour ne fournit pas intrinsèquement une défense contre toute menace identifiée; il s'agit d'un mécanisme permettant de mettre en œuvre d'autres défenses au niveau de l'application. Il n'existe donc aucune exigence de sécurité spécifique pour un tel canal de retour.

7.3.7 Procédure d'identification

7.3.7.1 Généralités

Le paragraphe précédent a couvert les exigences relatives à l'identification des entités.

Les systèmes de transmission ouverts peuvent par ailleurs introduire le risque que des messages d'autres utilisateurs (inconnus) soient confondus avec les informations provenant de la source voulue (il s'agit d'une forme de mascarade).

Une procédure d'identification conçue de manière appropriée au sein du processus relatif à la sécurité peut fournir une défense contre cette menace.

Deux types de procédures d'identification peuvent être distingués.

- Identification bidirectionnelle
  Lorsqu'un canal de communication en retour est disponible, l'échange des identifiants d'entités entre émetteurs et récepteurs des informations peut fournir une garantie supplémentaire que la communication s'effectue bien entre les partenaires souhaités.
- Procédures d'identification dynamique
  L'échange dynamique d'informations entre les émetteurs et les récepteurs, y compris la transformation et le retour à l'émetteur sur les informations reçues, peut permettre de garantir que les partenaires de la communication ne se contentent pas de déclarer avoir la bonne identité, mais également qu'ils se comportent de la manière attendue. Ce type de procédure d'identification peut être utilisé pour préfacer la transmission d'informations entre des processus relatifs à la sécurité qui communiquent et/ou il peut être utilisé au cours de la transmission d'informations elle-même.

7.3.7.2 Exigences

La procédure d'identification fait partie du processus d'application relatif à la sécurité. Les exigences détaillées doivent être définies dans la spécification des exigences de sécurité.

7.3.8 Code de sécurité

7.3.8.1 Généralités

En général, dans les systèmes de transmission, les codes de transmission sont utilisés pour détecter des erreurs aléatoires ou des paquets d'erreurs et/ou pour améliorer la qualité de transmission à l'aide de techniques de correction d'erreurs. Bien que ces codes de transmission puissent être très efficaces, ils peuvent échouer en raison de défauts matériels, d'influences externes ou d'erreurs systématiques.

Le processus relatif à la sécurité ne doit pas se fier à ces codes de transmission du point de vue de la sécurité. Un code de sécurité sous contrôle du processus relatif à la sécurité est donc par ailleurs exigé pour détecter la corruption des messages.

Le dossier de sécurité doit démontrer le caractère approprié des éléments suivants par rapport au niveau d'intégrité de la sécurité exigé et la nature des fonctions relatives à la sécurité:

- la capacité de détection des types de corruption systématique de messages attendus;
- la probabilité de détection des types de corruption aléatoire de messages.

NOTE Le code de sécurité peut être une combinaison de différents codes, par exemple un code linéaire combiné à une valeur constante.

Des lignes directrices pour la sélection des codes de sécurité sont données à l'Article C.3.

7.3.8.2 Exigences

7.3.8.2.1 Le code de sécurité doit être différent du code de transmission, sauf si l'intégrité du message est assurée uniquement par le code de sécurité. Cette différence peut être obtenue:

- soit en utilisant des algorithmes différents, soit
- en utilisant des paramètres de configuration différents (par exemple les polynômes) pour les mêmes algorithmes. Si les deux codes sont basés sur un CRC, les polynômes doivent être différents. Si les deux polynômes ont des facteurs communs, leur contribution à la performance du code de sécurité doit être négligée dans l'analyse de sécurité.

Dans le cas d'un système de transmission fermé, le concepteur peut simplement choisir un code de sécurité différent du code de transmission car il dispose d'une connaissance totale du système de transmission. Dans le cas d'un système de transmission ouvert, cette exigence peut être satisfaite en utilisant un code de sécurité qui n'est pas utilisé par les systèmes de transmission commerciaux.

7.3.8.2.2 Le code de sécurité doit détecter:

- les erreurs de transmission, par exemple provoquées par des perturbations électromagnétiques,
- les erreurs systématiques causées par des défaillances de matériel au sein du système de transmission non fiable.

Les défaillances imitant le code de sécurité ne peuvent pas être détectées correctement. Le code de sécurité doit donc être plus complexe que les défaillances potentielles. Ainsi il peut être supposé qu'une défaillance de matériel dans le système de transmission non fiable ne peut pas générer un code de sécurité valide.

7.3.8.2.3 Pour réaliser l'intégrité de sécurité exigée, il est nécessaire que le code de sécurité soit suffisamment complexe, par exemple basé sur un CRC, pour détecter et réagir aux défauts et erreurs typiques. L'analyse doit inclure au minimum:

- interruption de la ligne de transmission;
- toutes les logiques de bits 0;
- toutes les logiques de bits 1;
- inversion de message;
- décalage de synchronisation (en cas de transmission sérielle);
- erreurs aléatoires;
- paquets d'erreurs;
- erreurs systématiques, par exemple modèles d'erreurs répétés;
- combinaison des éléments ci-dessus.

7.3.8.2.4 L'analyse probabiliste des performances du code de sécurité doit être compatible avec l'objectif de sécurité. Un modèle des modes de défaillance doit être fourni et toutes les suppositions faites pour les calculs doivent être vérifiées et validées.

La probabilité d'erreurs non détectées des codes linéaires est souvent calculée en utilisant le modèle BSC (canal binaire symétrique), voir l'Article C.4. Si le code non binaire est utilisé le QSC (canal q-aire symétrique) peut être plus approprié. La présente norme recommande de limiter cette probabilité à la valeur dans le pire des cas calculée par ces modèles.

Le BSC est adapté aux erreurs aléatoires, telles que celles causées par les EMI. Cependant les erreurs aléatoires simples sont ordinairement éliminées par le système de transmission non fiable. Si une erreur est détectée par le code de sécurité, plusieurs bits du message relatif à la sécurité sont donc perturbés d'ordinaire. Etant donné qu'aucun modèle simple n'est disponible pour ces cas, la présente norme recommande de ne pas utiliser de probabilités d'erreurs non détectées inférieures à la valeur dans le pire des cas obtenue par l'application du BSC pour un taux d'erreur inférieur à la moitié (voir l'Article C.4).

Un exemple de modèle simplifié pour un système de transmission fermé est donné à l'Article C.4 (informatif).

7.3.9 Techniques cryptographiques

7.3.9.1 Généralités

Les techniques cryptographiques peuvent être utilisées si des attaques malveillantes au sein du réseau de transmission ouvert ne peuvent pas être exclues.

C'est généralement le cas lorsque la communication relative à la sécurité recourt à:

- un réseau public,
- un système de transmission radio,
- un système de transmission ayant des connexions avec des réseaux publics.

Pour faire face aux attaques intentionnelles exécutées à l'aide de messages envoyés aux applications relatives à la sécurité, les messages relatifs à la sécurité doivent être protégés par des techniques cryptographiques.

Cette exigence visant à éviter les mascarades de la part d'émetteurs non autorisés, peut être satisfaite grâce à l'une des solutions suivantes:

a) utiliser un code de sécurité capable de fournir une protection cryptographique;

b) crypter les messages après l'application du code de sécurité;

c) ajouter un code cryptographique au code de sécurité.

Ces techniques peuvent être combinées avec le mécanisme d'encodage de sécurité ou ajoutées séparément. L'Annexe C présente quelques solutions possibles.

Les techniques cryptographiques impliquent l'utilisation de clés et d'algorithmes. Le degré d'efficacité dépend de la force des algorithmes et du caractère secret des clés. Le caractère secret d'une clé dépend de sa longueur et de sa gestion.

7.3.9.2 Exigences

Le dossier de sécurité doit démontrer le caractère approprié des éléments suivants par rapport au niveau d'intégrité de la sécurité du processus et la nature du processus relatif à la sécurité:

- choix technique des techniques cryptographiques, y compris
  - performance de l'algorithme de cryptage (par exemple symétrique ou asymétrique),
  - caractéristiques de la clé (par exemple fixe ou basée sur la session),
  - justification de la longueur de clé sélectionnée,
  - fréquence de mise à jour de la clé,
  - stockage physique des clés,
- choix technique des architectures cryptographiques, y compris
  - vérification du bon fonctionnement (avant et pendant la phase opérationnelle) des processus cryptographiques lorsqu'ils sont mis en œuvre hors de l'équipement relatif à la sécurité,
- activités de gestion, y compris
  - production, stockage, distribution et révocation des clés confidentielles,
  - gestion des équipements,
  - processus de révision de l'adéquation des techniques cryptographiques avec le risque d'attaques malveillantes.

L'algorithme cryptographique doit être appliqué à toutes les données utilisateur et peut être appliqué à des données additionnelles qui ne sont pas transmises, mais sont connues de l'émetteur et du récepteur (données implicites).

Des hypothèses raisonnables doivent être formulées sur la nature, la motivation, les moyens financiers et techniques d'un attaquant potentiel et prendre également en compte les développements (à la fois techniques, comme l'augmentation de la puissance des ordinateurs, la diminution du coût des processeurs rapides, la diffusion des connaissances sur les algorithmes, et "sociaux" comme des conflits économiques, une aggravation du vandalisme, etc.) qui peuvent se produire au cours de la vie du système.

Pour la gestion des clés, des techniques normalisées sont fortement recommandées (par exemple conformément à la série ISO/IEC 11770).

7.4 Applicabilité des défenses

7.4.1 Généralités

Les défenses présentées en 7.3 peuvent être relatives à l'ensemble des menaces possibles défini à l'Article 5. Chaque défense peut fournir une protection contre une ou plusieurs menaces pesant sur la transmission. Dans le dossier de sécurité, on doit démontrer qu'il existe au moins une défense ou combinaison de défenses pour chacune des menaces possibles définies.

7.4.2 Matrice des menaces/défenses

Les X du Tableau 1 indiquent qu'une défense peut fournir une protection contre la menace correspondante. Les défenses du Tableau 1 peuvent être étendues conformément à 7.2.7.

Tableau 1 – Matrice des menaces/défenses

Menaces	Défenses							
	Numéro de séquence	Datation	Tempo-risation	Identificateurs de source et de destination	Message en retour	Procédure d'identifica-tion	Code de sécurité	Techniques cryptographiques
Répétition	X	X						
Suppression	X							
Insertion	X			X[a]	X [b]	X [b]		
Reséquencement	X	X						
Corruption							X [c]	X
Retard		X	X					
Mascarade					X [b]	X [b]		X [c]

[a] Seulement applicable pour l'identifiant de la source.
Ne détectera que les insertions à partir d'une source invalide.
Si des identifiants uniques ne peuvent pas être déterminés à cause d'utilisateurs inconnus, une technique cryptographique doit être utilisée, voir 7.3.9.

[b] Selon l'application.

[c] Voir 7.4.3 et Article C.2.

7.4.3 Choix et utilisation du code de sécurité et des techniques cryptographiques

Le choix du code de sécurité et des techniques cryptographiques doit être déterminé par les éléments suivants:

- le fait que l'accès non autorisé peut ou non être exclu;
- le type de code cryptographique proposé;
- la séparation ou non de la protection d'accès relative à la sécurité des processus relatifs à la sécurité.

Des lignes directrices concernant ces problèmes sont données à l'Article C.2.

Annexe A
(informative)

Menaces auxquelles sont exposés les systèmes de transmission ouverts

A.1 Vue générale

Les menaces auxquelles sont exposés les messages envoyés sur la liaison par le système de commande et de protection sont dues aux éventuels changements qui affectent les performances de la liaison et qui peuvent se produire soit dans des conditions normales (c'est-à-dire sans défaillance) soit dans des conditions anormales (c'est-à-dire suite à des défaillances dans le système de transmission).

L'approche retenue pour déduire une série de menaces consiste à fractionner en trois niveaux distincts l'analyse du danger réalisée sous forme d'arbre (voir Figure A.1):

- le niveau de l'utilisateur;
- le niveau du réseau;
- le niveau de l'environnement externe.

Ces niveaux suivent une approche descendante en partant du danger principal (MH) qui est l'impossibilité d'obtenir un message valide pour ce qui est de l'authenticité, l'intégrité, la succession et la rapidité au point de réception.

En analysant les comportements possibles du message côté réception, on a mis en évidence les situations de danger potentiel (dangers fondamentaux) et défini une série d'erreurs de messages fondamentales (BME), destinée à classer tous les modes possibles de défaillance des messages.

La déduction des menaces correspondantes est immédiate et représente les modes de défaillance du réseau (c'est-à-dire les erreurs de message du point du vue du réseau). La menace est l'entité à l'origine de la situation dangereuse pour la sécurité (c'est-à-dire une situation qui peut provoquer un accident) et représente (au niveau du réseau) une cause d'une éventuelle erreur fondamentale de message: la relation menaces-erreur fondamentale de message est donc 1:1.

Une menace peut elle-même être due à une série de causes, appelées événements dangereux (HE), qui peuvent se présenter soit au niveau du réseau soit au niveau de l'événement externe. Il est évident que le même événement dangereux peut être relatif à des menaces différentes.

Le fractionnement de l'analyse en plusieurs niveaux permet aussi de définir (au moins) trois niveaux de défense:

a) le niveau du système/application utilisateur, il s'agit là de la mise en œuvre du système indépendamment du champ de transmission, par exemple la suppression qui peut ne pas représenter de danger si le système a été conçu de telle manière que les messages supprimés ne représentent pas de danger;

b) la structure logique du message; par exemple tous les codes possibles qui peuvent être appliqués au message ou les contre-mesures spécifiques comme des numéros de séquence, des datations (horodatages), etc.;

c) le niveau physique; par exemple le blindage pour éviter une corruption par des interférences électromagnétiques.

La présente annexe ne traite pas en détail de ce sujet, mentionné dans le seul but de donner une représentation globale de la méthodologie utilisée.

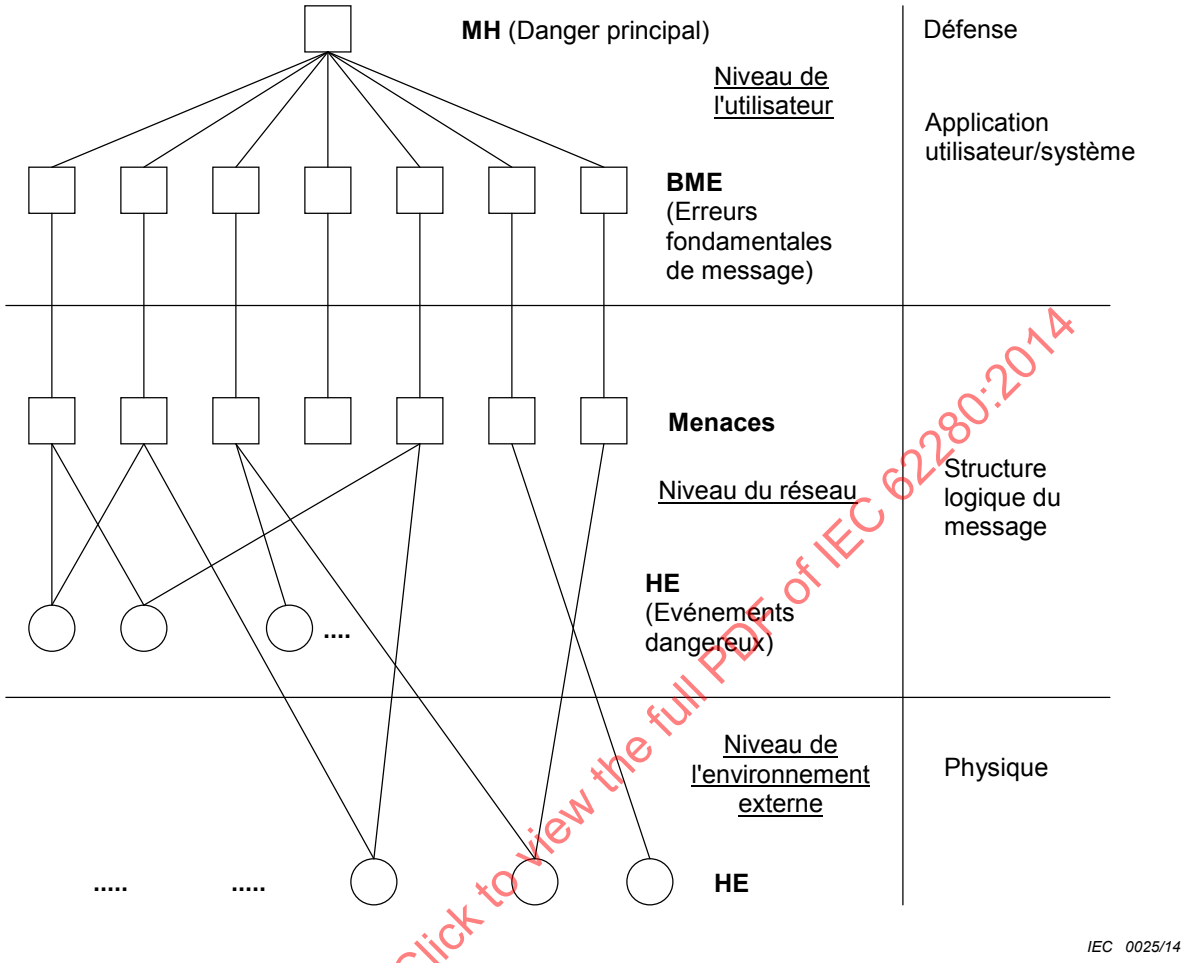


Figure A.1 – Arbre des dangers

A.2 Déduction des erreurs fondamentales de message

Le message constitue l'objet principal de toute l'analyse, le processus de communication a donc été observé du point de vue du récepteur. On peut définir un message comme “une information utile qui provient d'une source et doit être remise dans un délai Δt à compter du début de la transmission.”

C'est surtout l'intégrité du flux de messages qui permet d'identifier les dangers qui peuvent apparaître quand un message relatif à la sécurité est transmis dans un système de transmission ouvert.

Un "flux de messages" est défini comme une suite ordonnée de messages qui est unique pour chaque fenêtre temporelle et chaque récepteur dans un réseau s'il n'y a pas de défaillance, d'attaque ni d'opérations incorrectes.

Le flux de messages réellement reçu peut être différent de celui escompté pour un certain nombre de raisons. On distingue trois sous-classes particulières (dangers fondamentaux):

- davantage de messages reçus que de messages escomptés;
- moins de messages reçus que de messages escomptés;

- autant de messages reçus que de messages escomptés.

Davantage de messages reçus que de messages escomptés

Dans ce cas, un ou plusieurs messages ont été répétés ou un message extérieur a été inséré dans la ligne. Les erreurs fondamentales de message sont donc message répété, inséré.

Moins de messages reçus que de messages escomptés

Dans ce cas, un ou plusieurs messages ont été supprimés. L'erreur fondamentale de message est donc message supprimé.

Autant de messages reçus que de messages escomptés

Plusieurs choses peuvent alors se produire:

- tous les messages du flux ont un contenu et un temps de transfert corrects, mais l'ordre est faux: il y a eu ré-ordonnancement;
- un message du flux a mis plus de temps que le Δt nominal pour parvenir au récepteur: il y a eu retard;
- le message a été modifié: il y a eu corruption;
- le récepteur pense que l'expéditeur du message est différent de l'expéditeur réel: il y a eu usurpation d'identité.

Dans les deux derniers sous-cas, on a pris en compte l'intégrité du message unique. Les erreurs fondamentales de message sont message réordonné, retardé, corrompu, usurpé.

On a donc identifié l'ensemble suivant d'erreurs fondamentales de message:

- message répété;
- message supprimé;
- message inséré;
- message réordonné;
- message corrompu;
- message retardé;
- message usurpé.

Les erreurs fondamentales de message ci-dessus ne s'excluent pas l'une l'autre: il se peut que plusieurs messages d'un flux ou même un seul message soit affecté par plus d'un mode d'erreur.

A.3 Menaces

A.3.1 Généralités

Étant données les erreurs fondamentales de message présentées à l'Article A.2, on déduit immédiatement les menaces correspondantes.

On pose que A, B et C sont les trois parties autorisées qui échangent des messages relatifs à la sécurité tandis que X est l'attaquant.

A noter que la liste des menaces prend aussi en compte les défaillances logicielles/matérielles aléatoires et systématiques; les explications suivantes, données à titre d'exemple, ne sont donc pas exhaustives.

A.3.2 Répétition

– X copie un message [vitesse maximale: 250 km/h] et le duplique dans une situation inappropriée [alors que le train se trouve dans une section de voie à vitesse réduite],

ou

– après une défaillance HW, le système de transmission non sécurisé répète un message antérieur.

A.3.3 Suppression

– X supprime un message [X supprime un message Arrêt d'urgence ou Vitesse maximale: 250 km/h],

ou

– un message est supprimé à cause d'une défaillance HW.

A.3.4 Insertion

– X insère un message [vitesse maximale: 250 km/h],

ou

– un tiers autorisé C insère par inadvertance un message à l'intérieur du flux d'informations entre A et B (ou bien le même résultat est dû à une erreur réseau).

A.3.5 Reséquencement

– X modifie intentionnellement l'ordre des messages pour B (par exemple en retardant un message ou en forçant le message à suivre un autre chemin dans le réseau),

ou

– l'ordre du message change à cause d'une défaillance HW.

A.3.6 Corruption

– Le message est modifié accidentellement (par exemple perturbation électromagnétique) en un autre message dont la forme est correcte,

ou

– X altère un message [vitesse maximale: 30 km/h à Vitesse maximum: 250 km/h] de façon vraisemblable, si bien que A et/ou B ne peut pas détecter qu'il a été modifié.

A.3.7 Retard

– Le système de transmission est surchargé par le trafic normal (par exemple parce que la conception est mauvaise ou que le trafic a un niveau accidentellement élevé),

ou

– X crée une surcharge sur le système de transmission en produisant des messages factices pour retarder ou bloquer le service.

A.3.8 Mascarade

– A et B communiquent des données relatives à la sécurité,

et

– X déclare à A qu'il est B ou à B qu'il est A (ou les deux) pour avoir accès à des données relatives à la sécurité ou pour être considéré comme un utilisateur autorisé du système.

A.4 Approche possible pour élaborer un cas de sécurité

A.4.1 Généralités

L'approche qu'on va développer ci-dessous est un simple exemple; ce n'est pas la seule qu'on peut suivre. Une analyse complète des dangers exige qu'on connaisse très bien

l'application à laquelle elle s'applique pour qu'il soit possible de réaliser une évaluation correcte du risque.

A.4.2 Méthodes structurées pour identifier les événements dangereux

A.4.2.1 Généralités

Dans ce qui suit, l'analyse part du principe que le cas examiné concerne un réseau qui interagit avec un environnement extérieur. Ces deux entités se composent de sous-entités (présentées à la Figure A.2) qui peuvent être considérées comme la cause des événements dangereux possibles dans le système analysé. L'entité du réseau est divisée conformément aux étapes de son cycle de vie et le fractionnement de l'environnement extérieur prend en compte deux caractéristiques: physique et humaine.

Les feuilles de l'arbre à la Figure A.2 représentent les causes de dangers: à chaque cause on identifie les événements dangereux possibles correspondants. Cette manière de procéder permet plus facilement d'attribuer une probabilité à chaque événement dangereux produit, du moment que la probabilité d'une cause unique est connue.

Dans ce qui suit, chaque cause est divisée en un certain nombre d'événements dangereux possibles; cette subdivision n'est pas exhaustive; on pourra retenir d'autres événements dangereux au cours de l'analyse des dangers en fonction de l'application particulière.

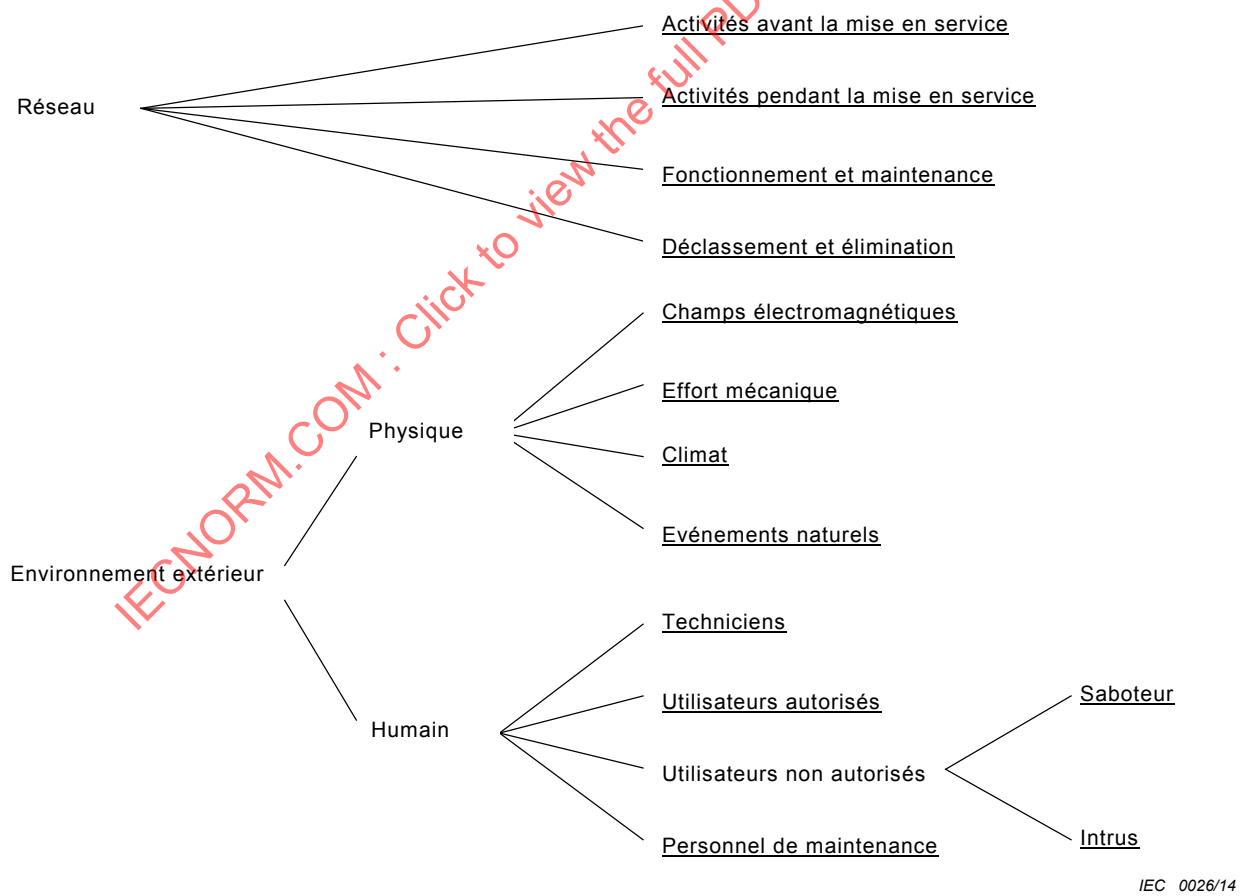


Figure A.2 – Causes de menaces

A.4.2.2 Réseau

A.4.2.2.1 Généralités

Les phases du cycle de vie du réseau peuvent être définies conformément à la CEI 62278. Dans le cadre de la présente annexe (où il s'agit d'identifier les événements dangereux dus à des "erreurs" à chaque phase), on peut les regrouper comme suit:

- conception, définition du système et conditions de l'application, analyse du risque, exigences du système, attribution des exigences du système, conception et mise en œuvre, fabrication; toutes ces phases sont relatives à des activités antérieures à la mise en service du système;
- installation, validation du système et acceptation du système: ces phases sont relatives à la mise en service du système;
- fonctionnement et maintenance;
- déclassement et élimination.

A.4.2.2.2 Activités avant la mise en service

Les erreurs pendant cette phase peuvent avoir pour conséquence:

- une défaillance HW systématique,
- une défaillance logicielle systématique.

A.4.2.2.3 Activités pendant la mise en service

Les erreurs pendant cette phase peuvent avoir pour conséquence:

- une paradiaphonie,
- une rupture des fils,
- un dépointage de l'antenne,
- des erreurs de câblage.

A.4.2.2.4 Fonctionnement et maintenance

Pendant cette phase du cycle, les événements dangereux peuvent être dus à des pertes de performance des composants du système et à des erreurs pendant les réparations et/ou les modifications:

- pertes de performance;
- défaillance aléatoire du matériel;
- vieillissement du matériel.

A.4.2.2.5 Maintenance

- utilisation d'instruments non étalonnés;
- utilisation d'instruments inadaptés;
- remplacement incorrect du matériel;
- mise à niveau ou remplacement incorrect des logiciels.

A.4.2.2.6 Modification

- effets d'évanouissement;
- erreurs humaines [1].

[1] Comme elles dépendent du type particulier de l'application, on ne peut pas les spécifier à ce niveau de l'analyse.

A.4.2.2.7 Déclassement et élimination

On ne considère pas que des événements dangereux relatifs à la communication puissent arriver pendant cette phase du cycle de vie d'un réseau.

A.4.2.3 Environnement extérieur

A.4.2.3.1 Champs électromagnétiques

- EMI (perturbation électromagnétique);
- diaphonie (avec liaisons externes par câble ou radioélectriques).

A.4.2.3.2 Effort mécanique

- défaillances aléatoires du matériel;
- vieillissement du matériel.

A.4.2.3.3 Climat

- bruit thermique;
- vieillissement du matériel;
- défaillances aléatoires du matériel;
- effets d'évanouissement.

A.4.2.3.4 Evénements naturels

- orage magnétique;
- incendie;
- séisme;
- foudre.

A.4.2.3.5 Opérateurs

- erreurs humaines [1].

A.4.2.3.6 Utilisateurs autorisés

- erreurs humaines [1].
- surcharge du système de transmission.

A.4.2.3.7 Personnel de maintenance

- utilisation d'instruments non étalonnés;
- utilisation d'instruments inadaptés;
- remplacement incorrect du matériel;
- erreurs humaines [1];
- mise à niveau ou remplacement incorrect des logiciels.

A.4.2.3.8 Saboteur [2]

- écoute clandestine;
- dommages ou dégâts matériels ou changement de matériel;
- modifications logicielles non autorisées.

---

[2] Le saboteur et l'intrus sont tous deux des pirates, à la différence que le premier ne se soucie pas de ce qui est en ligne puisque son seul but est de modifier le réseau alors que le deuxième ne modifie pas le réseau, mais s'en sert pour obtenir des avantages.

A.4.2.3.9 Intrus [2]

- contrôle des canaux;
- transmission de messages non autorisés.

A.4.3 Relation entre les événements dangereux et les menaces

D'après l'Article A.1, on peut considérer que chaque menace est un ensemble d'événements dangereux qui la provoquent. A partir des événements dangereux qu'on a identifiés dans le paragraphe précédent, l'étape suivante consiste à élaborer une relation entre eux et les menaces présentées à l'Article A.3 par une méthode montante [3]. Le but est de vérifier qu'on ne trouve pas de menace supplémentaire afin de prouver que l'approche choisie est valide. Les relations entre les menaces et les événements dangereux peuvent être représentées au Tableau A.1.

Comme on peut le voir, on n'a trouvé aucune menace supplémentaire après avoir analysé chaque événement dangereux; on a ainsi la preuve que la liste de l'Article A.3 est exhaustive.

(Il doit être clair que le tableau ci-dessus ne prend en compte que les effets primaires pour chaque événement dangereux; en d'autres termes, on peut identifier d'autres relations.)

A.5 Récapitulatif

On a identifié deux approches différentes pour déduire l'ensemble des menaces possibles à une communication relative à la sécurité dans des systèmes de transmission. La première est une méthode descendante qui commence par le danger principal et se termine en classant tous les événements dangereux possibles qui sont à l'origine du danger. La deuxième commence par définir les deux principales entités du système en question (c'est-à-dire le réseau et l'environnement extérieur) pour classer les causes possibles des événements dangereux relatifs à ce système; ces événements sont ensuite associés à la ou aux menaces qu'ils entraînent.

Comme les deux analyses aboutissent au même ensemble de menaces, on peut utiliser les deux approches pour analyser les dangers dans les systèmes de transmission ouverts.

Tableau A.1 – Relation entre les événements dangereux et les menaces

Evénements dangereux	Menaces						
	Répétition	Suppression	Insertion	Reséquencement	Corruption	Retard	Mascarade
Défaillance HW systématique	X	X	X	X	X	X	
Défaillance logicielle systématique	X	X	X	X	X	X	
Paradiaphonie		X	X		X		
Rupture des fils		X			X	X	
Dépointage d'antenne		X			X		
Erreurs de câblage		X	X		X	X	
Défaillances aléatoires du matériel	X	X	X	X	X	X	

[3] De façon générale, il convient d'utiliser une telle méthode ascendante pendant l'analyse de la sécurité pour évaluer les menaces dues à tous les événements dangereux relatifs à l'application particulière.

Evénements dangereux	Menaces						
	Répétition	Suppression	Insertion	Reséquencement	Corruption	Retard	Mascarade
Vieillissement du matériel	X	X	X	X	X	X	
Utilisation d'instruments non étalonnés	X	X	X	X	X	X	
Utilisation d'instruments inadaptés	X	X	X	X	X	X	
Remplacement incorrect du matériel	X	X	X	X	X	X	
Effets d'évanouissement		X		X	X	X	
Perturbation électromagnétique		X			X		
Erreurs humaines	X	X	X	X	X	X	
Bruit thermique		X			X		
Orage magnétique		X			X	X	
Feu.		X			X	X	
Tremblement de terre		X			X	X	
Foudre		X			X	X	
Surcharge du système de transmission		X				X	
Ecoute clandestine	X	X	X	X	X	X	
Dommages ou dégâts matériels		X			X	X	
Modifications logicielles non autorisées	X	X	X	X	X	X	X[a]
Transmission de messages non autorisés	X		X				X[a]
Contrôle des canaux [b]							

[a] Dans ce cas, le message est frauduleux dès le début, une défense stricte est nécessaire, par exemple l'utilisation d'une clé.

[b] Un contrôle non autorisé des messages relatifs à la sécurité n'est pas considéré directement comme un événement dangereux; le système court un danger à cause de la "transmission de messages non autorisés" dus à un contrôle non autorisé. La confidentialité des données de l'application est une autre exigence du système qui n'entre pas dans le domaine d'application de la présente norme.

Annexe B
(informative)

Catégories de systèmes de transmission

B.1 Catégories de systèmes de transmission

Le paragraphe 6.3 identifie trois catégories de systèmes de transmission.

- Catégorie 1 - Systèmes de transmission fermés, dans lesquels toutes les propriétés vitales du système sont contrôlées par le concepteur du système relatif à la sécurité et pour lequel on peut définir un ensemble simplifié d'exigences de sécurité;
- Catégorie 2 - Systèmes de transmission ouverts, dans lesquels on peut considérer comme négligeable le risque d'attaque malveillante bien que la transmission ne soit pas entièrement contrôlée par le concepteur du système relatif à la sécurité;
- Catégorie 3 - Systèmes de transmission ouverts, dans lesquels le risque danger d'attaque est possible et dans lesquels des mesures de défense cryptographiques sont exigées.

Le Tableau B.1 ci-dessous donne quelques indications supplémentaires pour répartir dans l'une des trois catégories ci-dessus les systèmes réels de transmission qu'on peut rencontrer dans les applications relatives à la sécurité, en se fondant sur les caractéristiques de la technologie à laquelle ils ont recours et sur les principales fonctionnalités de leur configuration.

Il n'est pas possible d'être précis en prenant des systèmes purement hypothétiques à titre d'exemple; les principales caractéristiques qui figurent dans le tableau peuvent cependant être utiles aux utilisateurs de cette norme pour déterminer s'il convient de considérer qu'un système donné ressortit de la catégorie 1, 2 ou 3 pour les besoins de l'analyse.

Tableau B.1 – Catégories de systèmes de transmission

Catégorie	Principales caractéristiques	Exemples de systèmes de transmission
Catégorie 1	Conçu pour des participants connus dont le nombre maximal est fixé. Toutes les propriétés du système de transmission sont connues, elles ne changent pas au cours du cycle de vie du système. La possibilité d'accès non autorisé est négligeable.	Transmission proche de l'entrefer (par exemple de balise de la voie à l'antenne du train). Bus en série interne de marque dans le système relatif à la sécurité - par exemple PROFIBUS, CAN, MVB (bus de véhicule multifonctions, défini par la CEI). Réseau local industriel normalisé qui relie plusieurs équipements (relatifs à la sécurité et non relatifs à la sécurité) à l'intérieur d'un seul système dont les préconditions sont soumises à exécution et à maintenance.
Catégorie 2	Les propriétés sont inconnues, en partie inconnues ou changent pendant le cycle de vie du système. Peu de possibilités d'étendre le groupe d'utilisateurs. Le ou les groupes d'utilisateurs sont connus. La possibilité d'accès non autorisé est négligeable (les réseaux sont sécurisés). Utilisation occasionnelle de réseaux non sécurisés.	Bus en série interne de marque dans le système relatif à la sécurité (par exemple PROFIBUS, MVB), mais il est possible de reconfigurer ou de remplacer le système de transmission par un autre pendant le cycle de vie. Réseau local industriel normalisé qui relie plusieurs équipements (relatifs à la sécurité et non relatifs à la sécurité) dans une zone contrôlée et limitée. Réseau étendu qui appartient au chemin de fer et relie différents systèmes (relatifs à la sécurité et non relatifs à la sécurité) à plusieurs endroits. Circuit commuté dans le réseau téléphonique public, utilisé occasionnellement à des moments impossibles à prévoir (par exemple diagnostic de commutation à distance pour un système de verrouillage). Circuit spécialisé permanent point à point dans le réseau téléphonique public. Système de transmission radio à accès restreint (par exemple utilisation de guides d'ondes ou de câbles à fuite quand le budget de liaison permet seulement la réception par un émetteur-récepteur proche ou utilise un schéma de modulation de marque, impossible à reproduire par un équipement de laboratoire conventionnel ou bon marché).
Catégorie 3	Les propriétés sont inconnues, en partie inconnues ou changent pendant le cycle de vie du système. Les groupes d'utilisateurs nombreux sont inconnus. La possibilité d'accès non autorisé est significative.	Données commutées par paquets dans le réseau téléphonique public. Internet. Données radio commutées par circuit (par exemple GSM-R). Données radio commutées par paquets (par exemple GPRS). Radiodiffusion à courte distance (par exemple Wi-Fi). Systèmes de radiotransmission sans restriction

B.2 Relations entre les catégories de systèmes de transmission et les menaces

Le Tableau B.2 ci-dessous est une simple attribution de menaces à chaque catégorie de systèmes de transmission telles qu'elles sont définies ci-dessus.